A zero-one law for the existence of triangles in random key graphs

Osman Yağan and Armand M. Makowski*
oyagan@umd.edu, armand@isr.umd.edu
Department of Electrical and Computer Engineering
and Institute for Systems Research
University of Maryland, College Park, MD 20742.

October 2, 2009

Abstract

Random key graphs are random graphs induced by the random key predistribution scheme of Eschenauer and Gligor under the assumption of full visibility. For this class of random graphs we show the existence of a zero-one law for the appearance of triangles, and identify the corresponding critical scaling. This is done by applying the method of first and second moments to the number of triangles in the graph.

Keywords: Wireless sensor networks, Key predistribution, Random key graphs, Zero-one laws, Existence of triangles.

1 Introduction

Random key graphs are random graphs that belong to the class of random intersection graphs [13]; in fact they are sometimes called uniform random intersection graphs by some authors [6, 7]. They have appeared recently in application areas as diverse as clustering analysis [6, 7], collaborative filtering in recommender systems [10] and random key predistribution for wireless sensor networks (WSNs) [4]. In this last context, random key graphs naturally occur in the study of the following random key predistribution

*This work was supported by NSF Grant CCF-07290.

scheme introduced by Eschenauer and Gligor [4]: Before deployment, each sensor in a WSN is independently assigned K distinct cryptographic keys which are selected at random from a pool of P keys. These K keys constitute the key ring of the node and are inserted into its memory. Two sensor nodes can then establish a secure link between them if they are within transmission range of each other and if their key rings have at least one key in common; see [4] for implementation details. If we assume *full visibility*, namely that nodes are all within communication range of each other, then secure communication between two nodes requires only that their key rings share at least one key. The resulting notion of adjacency defines the class of random key graphs; see Section 2 for precise definitions.

Much efforts have recently been devoted to developing zero-one laws for the property of connectivity in random key graphs. A key motivation can be found in the need to obtain conditions under which the scheme of Eschenauer and Gligor guarantees secure connectivity with high probability in large networks. An interesting feature of this work lies in the following fact: Although random key graphs are *not* equivalent to the classical Erdős-Rényi graphs [3], it is possible to transfer well-known zero-one laws for connectivity in Erdős-Rényi graphs to random key graphs by asymptotically matching their edge probabilities. This approach, which was initiated by Eschenauer and Gligor in their original analysis [4], has now been validated rigorously; see the papers [1, 2, 12, 15, 16] for recent developments. Furthermore, Rybarczyk [12] has shown that this transfer from Erdős-Rényi graphs also works for a number of issues related to the giant component and its diameter.

In view of these successes, it is natural to wonder whether the transfer technique can be applied to other graph properties. In particular, in the literature on random graphs there is a long standing interest [3, 8, 9, 11, 13] in the containment of certain (small) subgraphs, the simplest one being the *triangle*. This last case has some practical relevance since the number of triangles in a graph is closely related to its clustering properties [18]. With this in mind, we study the zero-one law for the existence of triangles in random key graphs and identify the corresponding critical scaling.

From these results we easily conclude that in the many node regime, the expected number of triangles in random key graphs is always at least as large as the corresponding quantity in asymptotically matched Erdős-Rényi graphs. For the parameter range that is of practical relevance in the context of WSNs, this expected number of triangles can be orders of magnitude larger in random key graphs than in Erdős-Rényi graphs, a fact also observed earlier via simulations in [2]. As a result, transferring results from Erdős-Rényi graphs by matching their edge probabilities is not a valid

approach in general, and can be quite misleading in the context of WSNs.

The zero-one laws obtained here were announced in the conference paper [17]. The results are established by making use of the method of first and second moments to the number of triangles in the graph. As the discussion amply shows, the technical details, especially for the one-law, are quite involved, and an outline of the proofs can be found in [17]. In line with developments currently available for other classes of graphs, e.g., Erdős-Rényi graphs [8, Chap. 3] and geometric random graphs [11, Chap. 3], it would be interesting to consider the containment problem for small subgraphs other than triangles other than triangle in the context of random key graphs. Given the difficulties encountered in the case of This is likely to be a challenging problem given the difficulties encountered in the simple case of triangles.

The paper is organized as follows: In Section 2 we formally introduce the class of random key graphs while in Section 3 we present the main results of the paper given as Theorem 3.1 and Theorem 3.2. Section 4 compares these results with the corresponding zero-one law in Erdős-Rényi graphs. The zero-one laws are established by an application of the method of first and second moments, respectively [8, p. 55]. To that end, in Section 5, we compute the expected value of the number of triangles in random key graphs. Asymptotic results to be used in the proofs of several results are then collected in Section 6 for easy reference. In Section 7.1, we give a proof of the zero-law (Theorem 3.1) while an outline for the proof of the one-law (Theorem 3.2) is provided in Section 7.2. The final sections of the paper, namely Sections 8 through 12, are devoted to completing the various steps of the proof of Theorem 3.2. Additional technical derivations are given in Appendices A, B and C.

A word on the notation and conventions in use: All limiting statements, including asymptotic equivalences, are understood with n going to infinity. The random variables (rvs) under consideration are all defined on the same probability triple $(\Omega, \mathcal{F}, \mathbb{P})$. Probabilistic statements are made with respect to this probability measure $\mathbb{P}$, and we denote the corresponding expectation operator by $\mathbb{E}$. The indicator function of an event E is denoted by $\mathbf{1}[E]$. For any discrete set S we write $|S|$ for its cardinality.

2 Random key graphs

The model is parametrized by the number n of nodes, the size P of the key pool and the size K of each key ring with $K \leq P$. We often group the integers P and K into the ordered pair $\theta \equiv (K, P)$ in order to simplify the

notation. Now, for each node $i = 1, \ldots, n$, let $K_i(\theta)$ denote the random set of K distinct keys assigned to node i and let $\mathcal{P}$ be the set of all keys. The rvs $K_1(\theta), \ldots, K_n(\theta)$ are assumed to be *i.i.d.* rvs, each of which is *uniformly* distributed with

$$\mathbb{P}\left[K_i(\theta) = S\right] = \binom{P}{K}^{-1}, \qquad i = 1, \ldots, n \tag{1}$$

for any subset S of $\mathcal{P}$ which contains exactly K elements. This corresponds to selecting keys randomly and *without* replacement from the key pool.

Distinct nodes $i, j = 1, \ldots, n$ are said to be adjacent if they share at least one key in their key rings, namely

$$K_i(\theta) \cap K_j(\theta) \neq \emptyset, \tag{2}$$

in which case an undirected link is assigned between nodes i and j. The resulting random graph defines the *random key graph* on the vertex set $\{1, \ldots, n\}$, hereafter denoted $\mathbb{K}(n; \theta)$.

For distinct $i, j = 1, \ldots, n$, it is easy to check that

$$\mathbb{P}\left[K_i(\theta) \cap K_j(\theta) = \emptyset\right] = q(\theta) \tag{3}$$

with

$$q(\theta) := \begin{cases} 0 & \text{if } \; P < 2K \\ \dfrac{\binom{P-K}{K}}{\binom{P}{K}} & \text{if } \; 2K \leq P, \end{cases} \tag{4}$$

whence the probability of edge occurrence between any two nodes is equal to $1 - q(\theta)$. The expression given in (4) is a simple consequence of the often used fact that

$$\mathbb{P}\left[S \cap K_i(\theta) = \emptyset\right] = \frac{\binom{P-|S|}{K}}{\binom{P}{K}}, \quad i = 1, \ldots, n \tag{5}$$

for every subset S of $\{1, \ldots, P\}$ with $|S| \leq P - K$. Note that if $P < 2K$ there exists an edge between any pair of nodes, so that $\mathbb{K}(n; \theta)$ coincides with the complete graph K_n. Also, we always have $0 \leq q(\theta) < 1$ with $q(\theta) > 0$ if and only if $2K \leq P$.

3 The main results

Pick positive integers K and P such that $K \leq P$. Fix $n = 3, 4, \ldots$ and for distinct $i, j, k = 1, \ldots, n$, define the indicator function

$$\chi_{n,ijk}(\theta) := \mathbf{1}\left[\text{Nodes } i, j \text{ and } k \text{ form a triangle in } \mathbb{K}(n; \theta)\right].$$

The number of (unlabelled) triangles in $\mathbb{K}(n;\theta)$ is simply given by

$$T_n(\theta) := \sum_{(ijk)} \chi_{n,ijk}(\theta) \tag{6}$$

where $\sum_{(ijk)}$ denotes summation over all distinct triples ijk with $1 \leq i < j < k \leq n$. The event $T(n,\theta)$ that there exists at least one triangle in $\mathbb{K}(n;\theta)$ is then characterized by

$$T(n,\theta) := [T_n(\theta) > 0] = [T_n(\theta) = 0]^c. \tag{7}$$

The main result of the paper is a zero-one law for the existence of triangles in random key graphs. To state these results we find it convenient to make use of the quantity

$$\tau(\theta) := \frac{K^3}{P^2} + \left(\frac{K^2}{P}\right)^3, \quad \theta = (K,P) \tag{8}$$

with positive integers K and P such that $K \leq P$. For simplicity of exposition we refer to any pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ as a *scaling* provided the natural conditions

$$K_n \leq P_n, \quad n = 2,3,\ldots \tag{9}$$

are satisfied. The zero-law is given first.

Theorem 3.1 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$, we have the zero-law*

$$\lim_{n\to\infty} \mathbb{P}\left[T(n,\theta_n)\right] = 0 \tag{10}$$

under the condition

$$\lim_{n\to\infty} n^3 \tau(\theta_n) = 0. \tag{11}$$

The one-law given next assumes a more involved form.

Theorem 3.2 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ for which the limit $\lim_{n\to\infty} q(\theta_n) = q^\star$ exists, we have the one-law*

$$\lim_{n\to\infty} \mathbb{P}\left[T(n,\theta_n)\right] = 1 \tag{12}$$

either if $0 \leq q^\star < 1$ or if $q^\star = 1$ under the condition

$$\lim_{n\to\infty} n^3 \tau(\theta_n) = \infty. \tag{13}$$

Theorem 3.1 and Theorem 3.2 will be established by the method of first and second moments, respectively [8, p. 55], applied to the count variables defined at (6). To facilitate comparison with Erdős-Rényi graphs, we combine Theorem 3.1 and Theorem 3.2 into a symmetric, but somewhat weaker, statement.

Theorem 3.3 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ for which $\lim_{n\to\infty} q(\theta_n) = 1$, we have*

$$\lim_{n\to\infty} \mathbb{P}\left[T(n;\theta_n)\right] = \begin{cases} 0 & \text{if } \lim_{n\to\infty} n^3\tau(\theta_n) = 0 \\ \\ 1 & \text{if } \lim_{n\to\infty} n^3\tau(\theta_n) = \infty. \end{cases} \tag{14}$$

4 Comparing with Erdős-Rényi graphs

In this section we compare Theorem 3.3 with its analog for Erdős-Rényi graphs. First some notation: For each p in $[0,1]$ and $n = 2, 3, \ldots$, let $\mathbb{G}(n;p)$ denote the Erdős-Rényi graph on the vertex set $\{1,\ldots,n\}$ with edge probability p. In analogy with (6) and (7) let $T_n(p)$ denote the number of (unlabelled) triangles in $\mathbb{G}(n;p)$, and define $T(n,p)$ as the event that there exists at least one triangle in $\mathbb{G}(n;p)$, i.e., $T(n,p) = [T_n(p) > 0]$. we also refer to any mapping $p : \mathbb{N}_0 \to [0,1]$ as a scaling for Erdős-Rényi graphs. The following zero-one law for connectivity in Erdős-Rényi graphs is well known [3].

Theorem 4.1 *For any scaling $p : \mathbb{N}_0 \to [0,1]$, we have*

$$\lim_{n\to\infty} \mathbb{P}\left[T(n;p_n)\right] = \begin{cases} 0 & \text{if } \lim_{n\to\infty} n^3\tau^\star(p_n) = 0 \\ \\ 1 & \text{if } \lim_{n\to\infty} n^3\tau^\star(p_n) = \infty \end{cases} \tag{15}$$

where

$$\tau^\star(p) := p^3, \quad p \in [0,1]. \tag{16}$$

As this result is also established by the method of first and second moments, its form is easily understood once we note that

$$\mathbb{E}\left[T_n(p)\right] = \binom{n}{3}\tau^\star(p), \quad 0 \le p \le 1 \tag{17}$$

for all $n = 3, 4, \ldots$.

As mentioned earlier, random key graphs are *not* equivalent to Erdős-Renyi graphs even when their edge probabilities are matched, i.e., $\mathbb{G}(n;p) \neq_{st} \mathbb{K}(n;\theta)$ with $p = 1 - q(\theta)$; see [17] for a discussion of similarities. However, in order to meaningfully compare the zero-one law of Theorem 4.1 with that contained in Theorem 3.3, we say that the scaling $p : \mathbb{N}_0 \to [0,1]$ (for Erdős-Rényi graphs) is *asymptotically matched* to the scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ (for random key graphs) if

$$p_n \sim 1 - q(\theta_n). \tag{18}$$

This is equivalent to requiring that the expected average degrees are asymptotically equivalent. Under the natural condition $\lim_{n\to\infty} q(\theta_n) = 1$, the matching condition (18) amounts to

$$p_n \sim \frac{K_n^2}{P_n} \tag{19}$$

by virtue of Lemma 6.1.

The definitions readily yield

$$\frac{\tau(\theta_n)}{\tau^\star(p_n)} = \frac{1}{p_n^3} \cdot \left(\frac{K_n^3}{P_n^2}\right) + \frac{1}{p_n^3} \cdot \left(\frac{K_n^2}{P_n}\right)^3, \quad n = 2, 3, \ldots$$

whence

$$\frac{\tau(\theta_n)}{\tau^\star(p_n)} \sim 1 + \frac{P_n}{K_n^3} \tag{20}$$

under (19). By Proposition 6.2, this last statement is equivalent to

$$\frac{\mathbb{E}\left[T_n(\theta_n)\right]}{\mathbb{E}\left[T_n(p_n)\right]} \sim 1 + \frac{P_n}{K_n^3} \tag{21}$$

as we make use of the expressions (17) and (30). In other words, for large n the expected number of triangles in random key graphs is always at least as large as the corresponding quantity in asymptotically matched Erdős-Rényi graphs.

In the context of WSNs, it is natural to select the parameters K_n and P_n of the scheme of Eschenauer and Gligor such that the induced random key graph is *connected*. However, there is a tradeoff between connectivity and security [2]. This requires that $\frac{K_n^2}{P_n}$ be kept as close as possible to the critical scaling $\frac{\log n}{n}$ for connectivity; see the papers [1, 2, 12, 15, 16]. In the desired near boundary regime, this amounts to

$$\frac{K_n^2}{P_n} \sim c \cdot \frac{\log n}{n} \tag{22}$$

with $c > 1$ but close to one, and from (21) we see that

$$\frac{\mathbb{E}\left[T_n(\theta_n)\right]}{\mathbb{E}\left[T_n(p_n)\right]} \sim 1 \quad \text{if and only if} \quad K_n \gg \frac{n}{\log n}. \tag{23}$$

The expected number of triangles in random key graphs is then of the same order as the corresponding quantity in asymptotically matched Erdős-Rényi graphs with $\mathbb{E}\left[T_n(\theta_n)\right] \sim \mathbb{E}\left[T_n(p_n)\right] \sim \frac{c^3}{6}\left(\log n\right)^3$. This conclusion holds regardless of the value of c in (22).

However, given the limited memory and computational power of the sensor nodes, the key ring sizes at (23) are not practical. In addition, they will lead to *high* node degrees and this in turn will decrease network *resiliency* against node capture attacks. Indeed, in [2, Thm. 5.3] it was proposed that security in WSNs be ensured by selecting K_n and P_n such that $\frac{K_n}{P_n} \sim \frac{1}{n}$, a requirement which then leads to

$$K_n \sim c \cdot \log n \tag{24}$$

under (22), and (21) implies

$$\lim_{n\to\infty} \frac{\mathbb{E}\left[T_n(\theta_n)\right]}{\mathbb{E}\left[T_n(p_n)\right]} = \lim_{n\to\infty} \left(1 + \frac{n}{(c \cdot \log n)^2}\right) = \infty. \tag{25}$$

Hence, for realistic WSN scenarios the expected number of triangles in the induced random key graphs can be orders of magnitude larger than in Erdős-Rényi graphs. This provides a clear example where transferring known results for Erdős-Rényi graphs to random key graphs by asymptotically matching their edge probabilities can be misleading.

5 Computing the first moment

With positive integers K and P such that $K \leq P$, define

$$\beta(\theta) := (1 - q(\theta))^3 + q(\theta)^3 - q(\theta)r(\theta) \tag{26}$$

where we have set

$$r(\theta) := \begin{cases} 0 & \text{if } \; P < 3K \\ \frac{\binom{P-2K}{K}}{\binom{P}{K}} & \text{if } \; 3K \leq P. \end{cases} \tag{27}$$

Direct inspection shows that

$$r(\theta) \leq q(\theta)^2 \tag{28}$$

whence

$$\beta(\theta) \geq (1 - q(\theta))^3 > 0. \tag{29}$$

Lemma 5.1 *For positive integers K and P such that $K \leq P$, we have*

$$\mathbb{E}\left[T_n(\theta)\right] = \binom{n}{3}\beta(\theta), \quad n = 3, 4, \ldots \tag{30}$$

To help deriving (30) we introduce the events

$$A(\theta) := [K_1(\theta) \cap K_2(\theta) \neq \emptyset] \cap [K_1(\theta) \cap K_3(\theta) \neq \emptyset] \tag{31}$$

and

$$\begin{aligned} B(\theta) &:= [K_1(\theta) \cap K_2(\theta) \neq \emptyset] \cap [K_1(\theta) \cap K_3(\theta) \neq \emptyset] \cap [K_2(\theta) \cap K_3(\theta) \neq \emptyset] \\ &= A(\theta) \cap [K_2(\theta) \cap K_3(\theta) \neq \emptyset]. \end{aligned} \tag{32}$$

The event $A(\theta)$ captures the existence of edges between node 1 and the pair of nodes 2 and 3, respectively, in $\mathbb{K}(n;\theta)$, while $B(\theta)$ is the event where the nodes 1, 2 and 3 form a triangle in $\mathbb{K}(n;\theta)$.

Lemma 5.2 *The probability of the event $A(\theta)$ is given by*

$$\mathbb{P}\left[A(\theta)\right] = (1 - q(\theta))^2. \tag{33}$$

In the proof of Lemma 5.2 (as well as in other proofs) we omit the explicit dependence on θ when no confusion arises from doing so.

Proof. Under the enforced independence assumptions we note that

$$\begin{aligned} \mathbb{P}\left[A(\theta)\right] &= \sum_{|S|=K} \mathbb{P}\left[K_1 = S, S \cap K_2 \neq \emptyset, S \cap K_3 \neq \emptyset\right] \\ &= \sum_{|S|=K} \mathbb{P}\left[K_1 = S\right] \mathbb{P}\left[S \cap K_2 \neq \emptyset\right] \mathbb{P}\left[S \cap K_3 \neq \emptyset\right] \\ &= (1 - q(\theta))^2 \end{aligned} \tag{34}$$

as we make use of (5) with $\sum_{|S|=K} \mathbb{P}\left[K_1 = S\right] = 1$. ■

In many of the forthcoming calculations we make repeated use of the fact that for any pair of events, say E and F, we have

$$\mathbb{P}\left[E \cap F\right] = \mathbb{P}\left[E\right] - \mathbb{P}\left[E \cap F^c\right]. \tag{35}$$

In particular, we can now conclude from Lemma 5.2 that

$$\begin{aligned} &\mathbb{P}\left[K_1(\theta) \cap K_2(\theta) = \emptyset,\ K_1(\theta) \cap K_3(\theta) \neq \emptyset\right] \\ &\quad = \ \mathbb{P}\left[K_1(\theta) \cap K_2(\theta) \neq \emptyset,\ K_1(\theta) \cap K_3(\theta) = \emptyset\right] \\ &\quad = \ q(\theta)(1 - q(\theta)) \end{aligned} \tag{36}$$

and

$$\mathbb{P}\left[K_1(\theta) \cap K_2(\theta) = \emptyset,\ K_1(\theta) \cap K_3(\theta) = \emptyset\right] = q(\theta)^2. \tag{37}$$

These facts will now be used in computing the probability of $B(\theta)$.

Lemma 5.3 *With $\beta(\theta)$ given at (26) we have*

$$\mathbb{P}\left[B(\theta)\right] = \beta(\theta). \tag{38}$$

Proof. Repeated use of (35) yields

$$\begin{aligned} \mathbb{P}\left[B(\theta)\right] \ &= \ \mathbb{P}\left[K_1 \cap K_2 \neq \emptyset,\ K_1 \cap K_3 \neq \emptyset\right] \\ &\qquad - \mathbb{P}\left[K_1 \cap K_2 \neq \emptyset,\ K_1 \cap K_3 \neq \emptyset,\ K_2 \cap K_3 = \emptyset\right] \\ &= \ \mathbb{P}\left[A(\theta)\right] - \mathbb{P}\left[K_1 \cap K_2 \neq \emptyset,\ K_2 \cap K_3 = \emptyset\right] \\ &\qquad + \mathbb{P}\left[K_1 \cap K_2 \neq \emptyset,\ K_1 \cap K_3 = \emptyset,\ K_2 \cap K_3 = \emptyset\right] \\ &= \ (1 - q(\theta))^2 - q(\theta)(1 - q(\theta)) + \mathbb{P}\left[K_1 \cap K_3 = \emptyset,\ K_2 \cap K_3 = \emptyset\right] \\ &\qquad - \mathbb{P}\left[K_1 \cap K_2 = \emptyset,\ K_1 \cap K_3 = \emptyset,\ K_2 \cap K_3 = \emptyset\right] \\ &= \ (1 - q(\theta))^2 - q(\theta)(1 - q(\theta)) + q(\theta)^2 \\ &\qquad - \mathbb{P}\left[K_1 \cap K_2 = \emptyset,\ K_1 \cap K_3 = \emptyset,\ K_2 \cap K_3 = \emptyset\right] \end{aligned} \tag{39}$$

as we recall (33), (36) and (37).

By independence we get

$$\begin{aligned} &\mathbb{P}\left[K_1 \cap K_2 = \emptyset,\ K_1 \cap K_3 = \emptyset,\ K_2 \cap K_3 = \emptyset\right] \\ &\quad = \ \mathbb{P}\left[K_1 \cap K_2 = \emptyset,\ (K_1 \cup K_2) \cap K_3 = \emptyset\right] \\ &\quad = \ \sum_{|S|=|T|=K, S \cap T = \emptyset} \mathbb{P}\left[K_1 = S, K_2 = T\right] \mathbb{P}\left[(S \cup T) \cap K_3 = \emptyset\right] \\ &\quad = \ \sum_{|S|=|T|=K, S \cap T = \emptyset} \mathbb{P}\left[K_1 = S, K_2 = T\right] \cdot r(\theta) \\ &\quad = \ \mathbb{P}\left[K_1 \cap K_2 = \emptyset\right] \cdot r(\theta) \end{aligned} \tag{40}$$

by invoking (5) (since $|S \cup T| = 2K$ under the constraints $|S| = |T| = K$ and $S \cap T = \emptyset$). Thus,

$$\mathbb{P}\left[B(\theta)\right] = (1 - q(\theta))^2 - q(\theta)(1 - q(\theta)) + q(\theta)^2 - q(\theta)r(\theta),$$

and the desired result follows upon noting the relation

$$(1 - q(\theta))^2 - q(\theta)(1 - q(\theta)) + q(\theta)^2 = (1 - q(\theta))^3 + q(\theta)^3.$$

■

The proof of Lemma 5.1 is now straightforward: Fix $n = 3, 4, \ldots$. Exchangeability yields

$$\mathbb{E}\left[T_n(\theta)\right] = \binom{n}{3} \mathbb{E}\left[\chi_{n,123}(\theta)\right] \tag{41}$$

and the desired conclusion follows as we make use of Lemma 5.3.

6 Some useful asymptotics

In this section we collect a number of asymptotic results that prove useful in establishing some of the results derived in this paper. The first result was already obtained in [16].

Lemma 6.1 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$, we have*

$$\lim_{n\to\infty} q(\theta_n) = 1 \tag{42}$$

if and only if

$$\lim_{n\to\infty} \frac{K_n^2}{P_n} = 0, \tag{43}$$

and under either condition the asymptotic equivalence

$$1 - q(\theta_n) \sim \frac{K_n^2}{P_n} \tag{44}$$

holds.

Since $1 \leq K_n \leq {K_n}^2$ for all $n = 1, 2, \ldots$, the condition (43) implies

$$\lim_{n\to\infty} \frac{K_n}{P_n} = 0 \tag{45}$$

and

$$\lim_{n\to\infty} P_n = \infty. \tag{46}$$

so that for any $c > 0$, we have

$$cK_n < P_n \tag{47}$$

for all n sufficiently large in $\mathbb{N}_0$ (dependent on c).

The following asymptotic equivalence will be crucial to stating the results in a more explicit form.

Proposition 6.2 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43), we have the asymptotic equivalence*

$$\beta(\theta_n) \sim \tau(\theta_n). \tag{48}$$

Proof. From (26), we get

$$\beta(\theta_n) = (1 - q(\theta_n))^3 + q(\theta_n)^3 \left(1 - \frac{r(\theta_n)}{q^2(\theta_n)}\right).$$

Under the enforced assumptions Lemma 6.1 already implies

$$(1 - q(\theta_n))^3 \sim \left(\frac{K_n^2}{P_n}\right)^3$$

with $q(\theta_n)^3 \sim 1$. It is now plain that the equivalence (48) will hold if we show that

$$1 - \frac{r(\theta_n)}{q(\theta_n)^2} \sim \frac{K_n^3}{P_n^2}. \tag{49}$$

This key technical fact is established in Appendix A. ■

The final result of this section also relies on Lemma 6.1, and will prove useful in establishing the one-law.

Proposition 6.3 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43), we have*

$$\lim_{n\to\infty} n^2(1 - q(\theta_n)) = \infty \tag{50}$$

provided the condition (13) holds.

Proof. Consider a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43). By Lemma 6.1 the desired conclusion (50) will be established if we show

$$\lim_{n\to\infty} n^2 \frac{K_n^2}{P_n} = \infty. \tag{51}$$

As condition (13) reads

$$\lim_{n\to\infty} n^3 \left(\frac{K_n^3}{P_n^2} + \left(\frac{K_n^2}{P_n} \right)^3 \right) = \infty,$$

we immediately get (51) from it by virtue of the trivial bounds

$$n^3 \left(\frac{K_n^2}{P_n} \right)^3 = \left(\frac{nK_n^2}{P_n} \right)^3 \leq \left(\frac{n^2 K_n^2}{P_n} \right)^3$$

and

$$n^3 \frac{K_n^3}{P_n^2} \leq n^4 \frac{K_n^4}{P_n^2} = \left(\frac{n^2 K_n^2}{P_n} \right)^2$$

valid for all $n = 1, 2, \ldots$. ■

Proposition 6.3 will be used as follows: Pick $a > 0$ and $b > 0$, and consider a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43). For each $n = 2, 3, \ldots$, we get

$$\begin{aligned} \frac{1}{n^2} \cdot \frac{(1 - q(\theta_n))^a}{\beta(\theta_n)^b} &\leq \frac{1}{n^2} \cdot \frac{(1 - q(\theta_n))^a}{(1 - q(\theta_n))^{3b}} \\ &= \frac{1}{n^2 (1 - q(\theta_n))} \cdot (1 - q(\theta_n))^{a-3b+1}. \end{aligned} \tag{52}$$

Therefore, under condition (13) Proposition 6.3 yields

$$\lim_{n\to\infty} \frac{1}{n^2} \cdot \frac{(1 - q(\theta_n))^a}{\beta(\theta_n)^b} = 0 \quad \text{if } a - 3b + 1 \geq 0 \tag{53}$$

as we make use of (42)-(43).

7 Proofs of Theorem 3.1 and Theorem 3.2

7.1 A proof of Theorem 3.1

Fix $n = 3, 4, \ldots$, An elementary bound for $\mathbb{N}$-valued rvs yields

$$\mathbb{P}\left[T_n(\theta_n) > 0\right] \leq \mathbb{E}\left[T_n(\theta_n)\right], \tag{54}$$

so that

$$\mathbb{P}\left[T(n, \theta_n)\right] \leq \binom{n}{3}\beta(\theta_n). \tag{55}$$

The conclusion (10) follows if we show that

$$\lim_{n\to\infty}\binom{n}{3}\beta(\theta_n) = 0 \tag{56}$$

under (11).

The condition $\lim_{n\to\infty} n^3\tau(\theta_n) = 0$ implies $\lim_{n\to\infty}\tau(\theta_n) = 0$ and (43) automatically holds. By Proposition 6.2 we conclude $\beta(\theta_n) \sim \tau(\theta_n)$, whence $n^3\beta(\theta_n) \sim n^3\tau(\theta_n)$, and condition (11) is indeed equivalent to (56) since $\binom{n}{3} \sim \frac{n^3}{6}$.

7.2 A proof of Theorem 3.2

Assume first that $q^\star$ satisfies $0 \leq q^\star < 1$. Fix $n = 3, 4, \ldots$ and partition the n nodes into the $k_n + 1$ non-overlapping groups $(1, 2, 3)$, $(4, 5, 6)$, …, $(3k_n + 1, 3k_n + 2, 3k_n + 3)$ with $k_n = \lfloor \frac{n-3}{3} \rfloor$. If $\mathbb{K}(n; \theta_n)$ contains no triangle, then *none* of these $k_n + 1$ groups of nodes forms a triangle. With this in mind we get

$$\begin{aligned}
&\mathbb{P}\left[T_n(\theta_n) = 0\right] \\
&\quad\leq \mathbb{P}\left[\bigcap_{\ell=0}^{k_n}\left[\begin{array}{c}\text{Nodes } 3\ell+1, 3\ell+2, 3\ell+3 \text{ do not form}\\ \text{a triangle in } \mathbb{K}(n;\theta_n)\end{array}\right]\right] \\
&\quad= \prod_{\ell=0}^{k_n}\mathbb{P}\left[\begin{array}{c}\text{Nodes } 3\ell+1, 3\ell+2, 3\ell+3 \text{ do not form}\\ \text{a triangle in } \mathbb{K}(n;\theta_n)\end{array}\right] \qquad (57)\\
&\quad= (1 - \beta(\theta_n))^{k_n+1} \\
&\quad\leq \left(1 - (1 - q(\theta_n))^3\right)^{k_n+1} \qquad (58)\\
&\quad\leq e^{-(k_n+1)(1-q(\theta_n))^3}. \qquad (59)
\end{aligned}$$

Note that (57) follows from the fact that the events

$$\left[\begin{array}{c}\text{Nodes } 3\ell+1, 3\ell+2, 3\ell+3 \text{ do not form} \\ \text{a triangle in } \mathbb{K}(n;\theta_n)\end{array}\right], \quad \ell = 0, \ldots, k_n$$

are mutually independent due to the non-overlap condition, while the inequality (58) is justified with the help of (29). Let n go to infinity in the inequality (59). The condition $q^\star < 1$ implies $\lim_{n\to\infty} \mathbb{P}\left[T(n,\theta_n)^c\right] = 0$ since $k_n \sim \frac{n}{3}$ so that $\lim_{n\to\infty}(k_n+1)(1-q(\theta_n))^3 = \infty$. This establishes (12).

To handle the case $q^\star = 1$, we use a standard bound which forms the basis of the method of second moment [8, remark 3.1, p. 55]. Here it takes the form

$$\frac{\mathbb{E}\left[T_n(\theta_n)\right]^2}{\mathbb{E}\left[T_n(\theta_n)^2\right]} \leq \mathbb{P}\left[T_n(\theta_n) > 0\right], \quad n = 3, 4, \ldots \tag{60}$$

It is now plain that (12) will be established in the case $q^\star = 1$ if we show the following result.

Proposition 7.1 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43), we have*

$$\lim_{n\to\infty} \frac{\mathbb{E}\left[T_n(\theta_n)^2\right]}{\mathbb{E}\left[T_n(\theta_n)\right]^2} = 1 \tag{61}$$

under the condition (13).

The remainder of the paper is devoted to establishing Proposition 7.1. As will soon become apparent this is a bit quite more involved than expected.

8 Computing the second moment

A natural step towards establishing Proposition 7.1 consists in computing the second moment of the count variables (6).

Proposition 8.1 *For positive integers K and P such that $K \leq P$, we have*

$$\begin{aligned}\mathbb{E}\left[T_n(\theta)^2\right] = \mathbb{E}\left[T_n(\theta)\right] \quad &+ \quad \left(\frac{\binom{n-3}{3}}{\binom{n}{3}} + 3\frac{\binom{n-3}{2}}{\binom{n}{3}}\right) \cdot \mathbb{E}\left[T_n(\theta)\right]^2 \\ &+ \quad \binom{n}{3}\binom{3}{2}\binom{n-3}{1} \cdot \mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,124}(\theta)\right]\end{aligned} \tag{62}$$

for all $n = 3, 4, \ldots$ *with*

$$\begin{aligned}
&\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,124}(\theta)\right] \\
&\quad = \quad -(1-q(\theta))^5 + 2\,(1-q(\theta))^2\,\beta(\theta) \\
&\qquad\quad - \frac{1}{q(\theta)}\left(\beta(\theta) - (1-q(\theta))^3\right)^2 + \sum_{k=0}^{K} c_k(\theta) - q(\theta)^4
\end{aligned} \tag{63}$$

where we have set

$$c_k(\theta) := \frac{\binom{K}{k}\binom{P-K}{K-k}}{\binom{P}{K}} \cdot \left(\frac{\binom{P-2K+k}{K}}{\binom{P}{K}}\right)^2, \quad k = 0, 1, \ldots, K. \tag{64}$$

A careful inspection of the definition (B.10) given for the quantities (64) yields the probabilistic interpretation

$$c_k(\theta) = \mathbb{P}\left[|K_1(\theta) \cap K_2(\theta)| = k, (K_1(\theta) \cup K_2(\theta)) \cap K_i(\theta) = \emptyset,\ i = 3, 4\right] \tag{65}$$

for each $k = 0, 1, \ldots, K$.

Proof. Consider positive integers K and P such that $K \leq P$ and fix $n = 3, 4, \ldots$. By exchangeability and by the binary nature of the rvs involved we readily conclude that

$$\begin{aligned}
\mathbb{E}\left[T_n(\theta)^2\right] &= \sum_{(ijk)}\sum_{(abc)} \mathbb{E}\left[\chi_{n,ijk}(\theta)\chi_{n,abc}(\theta)\right] \\
&= \mathbb{E}\left[T_n(\theta)\right] \\
&\quad + \binom{n}{3}\binom{3}{2}\binom{n-3}{1}\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,124}(\theta)\right] \\
&\quad + \binom{n}{3}\binom{3}{1}\binom{n-3}{2}\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,145}(\theta)\right] \\
&\quad + \binom{n}{3}\binom{n-3}{3}\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,456}(\theta)\right].
\end{aligned} \tag{66}$$

Under the enforced independence assumptions the rvs $\chi_{n,123}(\theta)$ and $\chi_{n,456}(\theta)$ are independent and identically distributed. As a result,

$$\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,456}(\theta)\right] = \mathbb{E}\left[\chi_{n,123}(\theta)\right]\mathbb{E}\left[\chi_{n,456}(\theta)\right] = \beta(\theta)^2$$

so that

$$\binom{n}{3}\binom{n-3}{3}\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,456}(\theta)\right] = \frac{\binom{n-3}{3}}{\binom{n}{3}} \cdot \mathbb{E}\left[T_n(\theta)\right]^2 \tag{67}$$

as we make use of the relation (30).

On the other hand, we readily check that the indicator rvs $\chi_{n,123}(\theta)$ and $\chi_{n,145}(\theta)$ are independent and identically distributed *conditionally* on $K_1(\theta)$ with

$$\mathbb{P}\left[\chi_{n,123}(\theta) = 1 | K_1(\theta) = S\right] = \mathbb{P}\left[\chi_{n,123}(\theta) = 1\right] = \beta(\theta), \quad S \in \mathcal{P}_K.$$

A similar statement applies to $\chi_{n,145}(\theta)$, and the rvs $\chi_{n,123}(\theta)$ and $\chi_{n,145}(\theta)$ are therefore (unconditionally) independent and identically distributed so that

$$\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,145}(\theta)\right] = \mathbb{E}\left[\chi_{n,123}(\theta)\right]\mathbb{E}\left[\chi_{n,145}(\theta)\right].$$

As before this last observation yields

$$\binom{n}{3}\binom{3}{1}\binom{n-3}{2}\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,145}(\theta)\right] = 3\frac{\binom{n-3}{2}}{\binom{n}{3}} \cdot \mathbb{E}\left[T_n(\theta)\right]^2 \tag{68}$$

by virtue of (30).

The evaluation (63)–(64) of the moment $\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,124}(\theta)\right]$ is rather lengthy, although quite straightforward; details are given in Appendix B. Reporting (63)–(64), (67) and (68) into (66) establishes Proposition 8.1. ■

In preparation of the proof of Proposition 7.1 we note that Proposition 8.1 readily implies

$$\begin{aligned} \frac{\mathbb{E}\left[T_n(\theta)^2\right]}{\mathbb{E}\left[T_n(\theta)\right]^2} = \frac{1}{\mathbb{E}\left[T_n(\theta)\right]} &+ \left(\frac{\binom{n-3}{3}}{\binom{n}{3}} + 3\frac{\binom{n-3}{2}}{\binom{n}{3}}\right) \\ &+ \frac{3(n-3)}{\binom{n}{3}} \cdot \frac{\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,124}(\theta)\right]}{\mathbb{E}\left[\chi_{n,123}(\theta)\right]^2} \end{aligned} \tag{69}$$

for all $n = 2, 3, \ldots$ as we make use of (41).

9 A proof of Proposition 7.1

Consider any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43). By Proposition 6.2 we have $\lim_{n\to\infty} n^3\beta(\theta_n) = \infty$ under the additional condition (13), whence

$$\lim_{n\to\infty} \mathbb{E}\left[T_n(\theta_n)\right] = \infty$$

by virtue of (41).

As pointed out earlier the equivalent conditions (42)-(43) imply

$$3K_n < P_n \tag{70}$$

for all n sufficiently large in $\mathbb{N}_0$. On that range (69) is valid with θ replaced by θ_n. Letting n go to infinity in the resulting expression, we note that

$$\lim_{n\to\infty}\left(\frac{\binom{n-3}{3}}{\binom{n}{3}}+3\frac{\binom{n-3}{2}}{\binom{n}{3}}\right)=1 \quad \text{and} \quad \frac{\binom{n}{3}}{3(n-3)}\sim\frac{n^2}{18}.$$

It is plain that the convergence (61) will hold if we show that

$$\lim_{n\to\infty}\frac{1}{n^2}\frac{\mathbb{E}\left[\chi_{n,123}(\theta_n)\chi_{n,124}(\theta_n)\right]}{\mathbb{E}\left[\chi_{n,123}(\theta_n)\right]^2}=0. \tag{71}$$

In order to establish (71) under the assumptions of Proposition 7.1 we proceed as follows: Recall from Lemma 5.1 that

$$\mathbb{E}\left[\chi_{n,123}(\theta_n)\right]^2=\beta(\theta_n)^2\geq\left(1-q(\theta_n)\right)^6, \tag{72}$$

and from (63) observe that

$$\begin{aligned}
&\frac{1}{n^2}\cdot\frac{\mathbb{E}\left[\chi_{n,123}(\theta_n)\chi_{n,124}(\theta_n)\right]}{\left(\mathbb{E}\left[\chi_{n,123}(\theta_n)\right]\right)^2}\\
&= -\frac{1}{n^2}\cdot\frac{\left(1-q(\theta_n)\right)^5}{\beta(\theta_n)^2}+\frac{2}{n^2}\cdot\frac{\left(1-q(\theta_n)\right)^2}{\beta(\theta_n)}\\
&\quad -\frac{1}{n^2}\cdot\frac{1}{q(\theta_n)}\left(\frac{\beta(\theta_n)-\left(1-q(\theta_n)\right)^3}{\beta(\theta_n)}\right)^2\\
&\quad +\frac{1}{n^2}\cdot\frac{\sum_{k=0}^{K_n}c_k(\theta_n)-q(\theta_n)^4}{\beta(\theta_n)^2}
\end{aligned} \tag{73}$$

for all $n=3,4,\ldots$.

Let n go to infinity in (73). Using (53) (once with $a=5$ and $b=2$, then with $a=2$ and $b=1$), we get

$$\lim_{n\to\infty}\frac{1}{n^2}\cdot\frac{\left(1-q(\theta_n)\right)^5}{\beta(\theta_n)^2}=0 \tag{74}$$

and

$$\lim_{n\to\infty}\frac{2}{n^2}\cdot\frac{\left(1-q(\theta_n)\right)^2}{\beta(\theta_n)}=0. \tag{75}$$

The convergence

$$\lim_{n\to\infty} \frac{1}{n^2} \cdot \frac{1}{q(\theta_n)} \left(\frac{\beta(\theta_n) - (1-q(\theta_n))^3}{\beta(\theta_n)} \right)^2 = 0 \tag{76}$$

is immediate since

$$\left| \frac{\beta(\theta_n) - (1-q(\theta_n))^3}{\beta(\theta_n)} \right|^2 \leq 1, \quad n = 2, 3, \ldots$$

and $\lim_{n\to\infty} q(\theta_n) = 1$. Consequently the proof of Proposition 7.1 will be completed if we show

Proposition 9.1 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43), we have*

$$\lim_{n\to\infty} \frac{1}{n^2} \cdot \frac{\sum_{k=0}^{K} c_k(\theta_n) - q(\theta_n)^4}{\beta(\theta_n)^2} = 0 \tag{77}$$

under the condition (13).

The proof of Proposition 9.1 will proceed in several steps which are presented in the next three sections.

10 The first reduction step

We start with an easy bound.

Lemma 10.1 *With positive integers K and P such that $2K \leq P$, we have*

$$c_1(\theta) \leq 1 - q(\theta). \tag{78}$$

Proof. Specializing (65) with $k = 1$ we get

$$\begin{aligned} c_1(\theta) &= \mathbb{P}\left[|K_1(\theta) \cap K_2(\theta)| = 1, (K_1(\theta) \cup K_2(\theta)) \cap K_i(\theta) = \emptyset,\ i = 3, 4\right] \\ &\leq \mathbb{P}\left[|K_1(\theta) \cap K_2(\theta)| = 1\right] \\ &\leq \mathbb{P}\left[|K_1(\theta) \cap K_2(\theta)| \geq 1\right] \end{aligned}$$

and the conclusion is immediate as we identify

$$\mathbb{P}\left[|K_1(\theta) \cap K_2(\theta)| \geq 1\right] = \mathbb{P}\left[K_1(\theta) \cap K_1(\theta) \neq \emptyset\right] = 1 - q(\theta).$$

■

Lemma 10.2 *With positive integers K and P such that $3K \leq P$, the monotonicity property*

$$\frac{c_1(\theta)}{c_0(\theta)} \geq \frac{c_2(\theta)}{c_1(\theta)} \geq \ldots \geq \frac{c_K(\theta)}{c_{K-1}(\theta)} \tag{79}$$

holds.

Proof. Fix $k = 0, \ldots, K-1$. From the expression (64) we note that

$$\begin{aligned} \frac{c_{k+1}(\theta)}{c_k(\theta)} &= \frac{\binom{K}{k+1}\binom{P-K}{K-k-1}\binom{P-2K+k+1}{K}^2}{\binom{K}{k}\binom{P-K}{K-k}\binom{P-2K+k}{K}^2} \\ &= \frac{1}{k+1} \cdot \frac{(K-k)^2}{P-3K+k+1} \cdot \frac{P-2K+k+1}{P-3K+k+1} \end{aligned} \tag{80}$$

and by considering each factor in this last expression we readily conclude that the ratio $\frac{c_{k+1}(\theta)}{c_k(\theta)}$ decreases monotonically with k. ■

Lemma 10.3 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43), we have*

$$\frac{c_2(\theta_n)}{c_1(\theta_n)} \leq 1 - q(\theta_n) \tag{81}$$

for all n sufficiently large in $\mathbb{N}_0$.

Proof. Pick a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43) so that (70) eventually holds. On that range replace θ by θ_n in (80) with $k = 1$ according to this scaling, yielding

$$\frac{c_2(\theta_n)}{c_1(\theta_n)} = \frac{1}{2} \cdot \frac{(K_n-1)^2}{P_n - 3K_n + 2} \cdot \frac{P_n - 2K_n + 2}{P_n - 3K_n + 2}.$$

The inequality

$$(1-q(\theta_n))^{-1} \frac{c_2(\theta_n)}{c_1(\theta_n)} \leq \frac{1}{2} \cdot (1-q(\theta_n))^{-1} \frac{K_n^2}{P_n - 3K_n} \cdot \frac{P_n - 2K_n}{P_n - 3K_n}$$

readily follows.

Now let n go to infinity in this inequality: Recall the consequence (45) of the assumption (42)-(43) and use the equivalence (44) to validate the limits

$$\lim_{n\to\infty} (1-q(\theta_n))^{-1} \frac{K_n^2}{P_n - 3K_n} = 1$$

and

$$\lim_{n\to\infty} \frac{P_n - 2K_n}{P_n - 3K_n} = 1.$$

As a consequence,

$$\limsup_{n\to\infty} (1-q(\theta_n))^{-1} \frac{c_2(\theta_n)}{c_1(\theta_n)} \leq \frac{1}{2}$$

and the desired conclusion is now immediate. ■

Combining Lemma 10.1, Lemma 10.2 and Lemma 10.3 will lead to the following key bounds.

Lemma 10.4 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43), we have*

$$c_k(\theta_n) \leq (1-q(\theta_n))^k, \quad k = 1, 2, \ldots, K_n \tag{82}$$

for all n sufficiently large in $\mathbb{N}_0$.

Proof. Pick a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43). For each $n = 2, 3, \ldots$, we can use Lemma 10.1 and Lemma 10.2 to conclude that

$$\begin{aligned} c_k(\theta_n) &= \prod_{\ell=1}^{k-1} \frac{c_{\ell+1}(\theta_n)}{c_\ell(\theta_n)} \cdot c_1(\theta_n) \\ &\leq \left(\frac{c_2(\theta_n)}{c_1(\theta_n)}\right)^{k-1} \cdot c_1(\theta_n) \\ &\leq \left(\frac{c_2(\theta_n)}{c_1(\theta_n)}\right)^{k-1} \cdot (1-q(\theta_n)) \end{aligned} \tag{83}$$

with $k = 1, \ldots, K_n$. The desired conclusion is now a simple consequence of Lemma 10.3. ■

We are now in a position to take the first step towards the proof of Proposition 9.1.

Proposition 10.5 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43), we have*

$$\lim_{n\to\infty} \frac{1}{n^2} \cdot \frac{\sum_{k=5}^{K_n} c_k(\theta_n)}{\beta(\theta_n)^2} = 0 \tag{84}$$

under the condition (13).

Proof. Pick a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43). The result (53) is trivially true if $K_n \leq 4$ for all n sufficiently large in $\mathbb{N}_0$. Thus, assume from now on that $K_n \geq 5$ for infinitely many n in $\mathbb{N}_0$ – In fact, there is now loss of generality in assuming $K_n \geq 5$ for all n sufficiently large in $\mathbb{N}_0$. From Lemma 10.4 it follows that

$$\begin{aligned} \sum_{k=5}^{K_n} c_k(\theta_n) &\leq \sum_{k=5}^{K_n} (1 - q(\theta_n))^k \\ &\leq \sum_{k=5}^{\infty} (1 - q(\theta_n))^k \\ &= \frac{(1 - q(\theta_n))^5}{q(\theta_n)} \end{aligned} \tag{85}$$

for all n sufficiently large in $\mathbb{N}_0$. Letting n go to infinity in this last inequality we readily obtain (84) as an immediate consequence of Proposition 6.3, to wit (53) (with $a = 5$ and $b = 2$). ■

11 The second reduction step

It is now plain from Proposition 10.5 that the proof of Proposition 9.1 will be completed if we show the following fact.

Proposition 11.1 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43), we have*

$$\lim_{n\to\infty} \frac{1}{n^2} \cdot \frac{\sum_{k=0}^{4} c_k(\theta_n) - q(\theta_n)^4}{\beta(\theta_n)^2} = 0 \tag{86}$$

under the condition (13).

To construct a proof of Proposition 11.1 we proceed as follows: Fix positive integers K and P such that $3K \leq P$. By direct substitution we get

$$\begin{aligned}
&\sum_{k=0}^{4} c_k(\theta) - q(\theta)^4 \\
&= \sum_{k=0}^{4} \frac{\binom{K}{k}\binom{P-K}{K-k}}{\binom{P}{K}} \left(\frac{\binom{P-2K+k}{K}}{\binom{P}{K}} \right)^2 - \left(\frac{\binom{P-K}{K}}{\binom{P}{K}} \right)^4 \\
&= \binom{P}{K}^{-4} \left(\sum_{k=0}^{4} \binom{P}{K}\binom{K}{k}\binom{P-K}{K-k}\binom{P-2K+k}{K}^2 - \binom{P-K}{K}^4 \right) \\
&= \frac{F(\theta)}{G(\theta)} \qquad (87)
\end{aligned}$$

where we have set

$$\begin{aligned}
&F(\theta) \qquad (88) \\
&:= (K!)^4 \left(\sum_{k=0}^{4} \binom{P}{K}\binom{K}{k}\binom{P-K}{K-k}\binom{P-2K+k}{K}^2 - \binom{P-K}{K}^4 \right)
\end{aligned}$$

and

$$G(\theta) := \left(\frac{P!}{(P-K)!} \right)^4 = \prod_{\ell=0}^{K-1} (P-\ell)^4. \qquad (89)$$

In this new notation Proposition 11.1 can be given a simpler, yet equivalent, form.

Proposition 11.2 *Consider any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43), The convergence (86) holds if and only if*

$$\lim_{n\to\infty} \frac{1}{n^2 \beta(\theta_n)^2} \frac{F(\theta_n)}{P_n^{4K_n}} = 0. \qquad (90)$$

Proof. Pick a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43) and assume that (13) holds. The desired equivalence is an immediate consequence of the expression (87) as we show below the equivalence

$$G(\theta_n) \sim P_n^{4K_n}. \qquad (91)$$

By (89) this last equivalence amounts to

$$\lim_{n\to\infty} \prod_{\ell=0}^{K_n-1} \left(\frac{P_n-\ell}{P_n}\right)^4 = 1. \tag{92}$$

To establish this convergence, fix $n = 2, 3, \ldots$ and note that

$$\prod_{\ell=0}^{K_n-1} \left(\frac{P_n-\ell}{P_n}\right)^4 = \left(\prod_{\ell=0}^{K_n-1} \left(1-\frac{\ell}{P_n}\right)\right)^4. \tag{93}$$

The bounds

$$\left(1-\frac{K_n}{P_n}\right)^{K_n} \le \prod_{\ell=0}^{K_n-1} \left(1-\frac{\ell}{P_n}\right) \le 1 \tag{94}$$

are straightforward, while simple calculus followed by a crude bounding rgument yields

$$1-\left(1-\frac{K_n}{P_n}\right)^{K_n} = \int_{1-\frac{K_n}{P_n}}^{1} K_n t^{K_n-1} dt \le \frac{K_n^2}{P_n}.$$

With the help of (94) we now conclude that

$$1-\frac{K_n^2}{P_n} \le \prod_{\ell=0}^{K_n-1} \left(1-\frac{\ell}{P_n}\right) \le 1. \tag{95}$$

Letting n go to infinity in this last expression yields the conclusion

$$\lim_{n\to\infty} \prod_{\ell=0}^{K_n-1} \left(1-\frac{\ell}{P_n}\right) = 1 \tag{96}$$

by virtue of (43), and this readily implies (92) via (93). ■

The following bound, which is established in Section 12, proves crucial for proving the convergence (90) under the assumptions of Proposition 11.1.

Lemma 11.3 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43), we have*

$$F(\theta_n) \le K_n^4 P_n^{4K_n-3} \tag{97}$$

for all n sufficiently large in $\mathbb{N}_0$.

While Lemma 11.3 is established in Section 12, the proof of Proposition 11.1 can now be completed: Pick a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43) and assume that (13) holds. By Lemma 11.3 we get

$$\frac{1}{n^2\beta^2(\theta_n)} \cdot \frac{F(\theta_n)}{P_n^{4K_n}} \leq \frac{1}{n^2\beta^2(\theta_n)} \cdot \frac{K_n^4}{P_n^3} \tag{98}$$

for all n sufficiently large in $\mathbb{N}_0$. Invoking Proposition 6.2 we then conclude that

$$\begin{aligned}
\frac{1}{n^2\beta^2(\theta_n)} \cdot \frac{K_n^4}{P_n^3} &\sim \frac{1}{n^2\tau(\theta_n)^2} \cdot \frac{K_n^4}{P_n^3} \\
&= \frac{K_n^4}{n^2 P_n^3 \left(\frac{K_n^3}{P_n^2} + \left(\frac{K_n^2}{P_n}\right)^3\right)^2} \\
&\leq \frac{K_n^4}{n^2 P_n^3 \left(\frac{K_n^3}{P_n^2}\right)^2} \\
&= \left(n^2 \frac{K_n^2}{P_n}\right)^{-1}. \qquad (99)
\end{aligned}$$

The validity of (90) follows upon letting n go to infinity in (98) and using (99) together with the consequence (51) of (13) discussed in the proof of Proposition 6.3. The proof of Proposition 11.1 is completed with the help of Proposition 11.2. ■

12 Towards Lemma 11.3

We are left with proving the key Lemma 11.3. To do so we will need to exploit the structure of $F(\theta)$: Thus, fix positive integers K and P such that $3K \leq P$, and return to (88). For each $k = 0, 1, \ldots, 4$, easy algebra shows that

$$\begin{aligned}
&(K!)^4 \binom{P}{K} \binom{K}{k} \binom{P-K}{K-k} \binom{P-2K+k}{K}^2 \\
&= \frac{P!}{k!(P-2K+k)!} \cdot \left(\frac{(K!)^2(P-2K+k)!}{K!(K-k)!(P-3K+k)!}\right)^2 \\
&= \frac{P!(P-2K+k)!}{k!} \cdot \left(\frac{K!}{(K-k)!(P-3K+k)!}\right)^2
\end{aligned}$$

$$= \quad k! \binom{K}{k}^2 \cdot b_{K,k}(\theta) \tag{100}$$

with

$$b_{K,k}(\theta) := \frac{P!(P-2K+k)!}{((P-3K+k)!)^2}. \tag{101}$$

Next, it is plain that

$$b_K(\theta) := (K!)^4 \binom{P-K}{K}^4 = \left(\frac{(P-K)!}{(P-2K)!} \right)^4. \tag{102}$$

Reporting these facts into (88) we readily conclude

$$\begin{aligned} F(\theta) &= \sum_{k=0}^{4} k! \binom{K}{k}^2 \cdot \frac{P!(P-2K+k)!}{((P-3K+k)!)^2} - \left(\frac{(P-K)!}{(P-2K)!} \right)^4 \\ &= \left(\sum_{k=0}^{4} k! \binom{K}{k}^2 \cdot b_{K,k}(\theta) \right) - b_K(\theta). \end{aligned} \tag{103}$$

By direct inspection, using (C.1) and (C.3) in Appendix C, we check that $F(\theta)$ can be written as a polynomial in P (of order $4K$), namely

$$F(\theta) = \sum_{\ell=0}^{4K} a_{4K-\ell}(K) P^{\ell} = \sum_{\ell=0}^{4K} a_{\ell}(K) P^{4K-\ell} \tag{104}$$

where the coefficients are *integers* which depend on θ only through K. The first six coefficients can be evaluated explicitly.

Lemma 12.1 *With positive integers K and P such that $3K \leq P$, we have*

$$a_0(K) = a_1(K) = a_2(K) = 0 \tag{105}$$

and

$$a_3(K) = K^4 \tag{106}$$

whereas

$$a_4(K) = -6K^6 + 6K^5 - K^4 \tag{107}$$

and

$$\begin{aligned} a_5(K) &= -\frac{1}{120}K^{10} + \frac{1}{6}K^9 + \frac{199}{12}K^8 - 34K^7 + \frac{1207}{120}K^6 \\ &\quad + \frac{161}{6}K^5 - \frac{209}{6}K^4 + 20K^3 - \frac{24}{5}K^2. \end{aligned} \tag{108}$$

The fact that (108) defines a polynomial expression in K with rational coefficients does not contradict the integer nature of $a_5(K)$. In what follows we shall find it convenient to write

$$a_5^\star(K) = a_5(K) + \frac{1}{240}K^{10}. \tag{109}$$

The proof of Lemma 12.1 is tedious and is given in Appendix C. For the remaining coefficients, we rely on the following bounds which are also derived in Appendix C.

Lemma 12.2 *With positive integers K and P such that $3K \le P$, we have*

$$|a_\ell(K)| \le 2 \cdot (12K^2)^\ell, \quad \ell = 0, 1, \ldots, 4K. \tag{110}$$

As expected these bounds are in agreement witht the exact expressions obtained in Lemma 12.1 for $\ell = 0, 1, \ldots, 5$.

A proof of Lemma 11.3 can now be given: Pick a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43) and replace θ by θ_n in (104) according to this scaling. As Lemma 12.1 implies

$$F(\theta_n) = K_n^4 P_n^{4K_n-3} + \sum_{\ell=4}^{4K_n} a_\ell(K_n) P_n^{4K_n-\ell} \tag{111}$$

for all $n = 2, 3, \ldots$, the bound (97) follows if we show that

$$\sum_{\ell=4}^{4K_n} a_\ell(K_n) P_n^{4K_n-\ell} \le 0 \tag{112}$$

for all n sufficiently large in $\mathbb{N}_0$.

To do so, apply (110) and use elementary arguments to get

$$\begin{aligned}
\left| \sum_{\ell=6}^{4K_n} a_\ell(K_n) P_n^{4K_n-\ell} \right| &\le \sum_{\ell=6}^{4K_n} |a_\ell(K_n)| \, P_n^{4K_n-\ell} \\
&\le \sum_{\ell=6}^{4K_n} 2 \cdot (12K_n^2)^\ell P_n^{4K_n-\ell} \\
&= 2P_n^{4K_n} \sum_{\ell=6}^{4K_n} \left(\frac{12K_n^2}{P_n} \right)^\ell
\end{aligned}$$

$$
\begin{aligned}
&\leq 2P_n^{4K_n}\left(\frac{12K_n^2}{P_n}\right)^6 \cdot \sum_{\ell=0}^{\infty}\left(\frac{12K_n^2}{P_n}\right)^{\ell} \\
&= 2P_n^{4K_n}\left(\frac{12K_n^2}{P_n}\right)^6 \cdot \left(1-\frac{12K_n^2}{P_n}\right)^{-1} \qquad (113)
\end{aligned}
$$

for all n large enough to ensure $12K_n^2 < P_n$, say $n \geq n_1^\star$ for some finite integer $n_1^\star$; this is a simple consequence of condition (42)-(43).

On that range, going back to (112), we find

$$
\begin{aligned}
&\sum_{\ell=4}^{4K_n} a_\ell(K_n)P_n^{4K_n-\ell} \\
&\leq a_4(K_n)P_n^{4K_n-4} + a_5(K_n)P_n^{4K_n-5} + \left|\sum_{\ell=6}^{4K_n} a_\ell(K_n)P_n^{4K_n-\ell}\right| \\
&\leq a_4(K_n)P_n^{4K_n-4} + a_5(K_n)P_n^{4K_n-5} + 2P_n^{4K_n}\left(\frac{12K_n^2}{P_n}\right)^6 \cdot \left(1-\frac{12K_n^2}{P_n}\right)^{-1} \\
&= P_n^{4K_n-5}\cdot L_n \qquad (114)
\end{aligned}
$$

where

$$
L_n := a_4(K_n)P_n + a_5(K_n) + 2(12)^6 K_n^{10}\cdot\frac{K_n^2}{P_n}\cdot\left(1-\frac{12K_n^2}{P_n}\right)^{-1}.
$$

Therefore, (112) will hold for all n sufficiently large in $\mathbb{N}_0$ provided

$$
L_n \leq 0 \qquad (115)
$$

for all n sufficiently large in $\mathbb{N}_0$. This last statement will be established by showing that $L = -\infty$ where

$$
L := \limsup_{n\to\infty} L_n.
$$

That $L = -\infty$ can be seen as follows: We begin with the bound

$$
a_4(K_n) = -K_n^4(6K_n(K_n-1)+1) \leq -K_n^4 \qquad (116)
$$

for all $n = 1, 2, \ldots$. Next, condition (42)-(43) implies

$$
\lim_{n\to\infty}\frac{K_n^2}{P_n}\cdot\left(1-\frac{12K_n^2}{P_n}\right)^{-1} = 0, \qquad (117)
$$

whence there exists some finite integer $n_2^\star$ such that

$$2(12)^6 \frac{K_n^2}{P_n} \cdot \left(1 - \frac{12K_n^2}{P_n}\right)^{-1} \leq \frac{1}{240}, \quad n \geq n_2^\star. \tag{118}$$

Now, set $n^\star = \max(n_1^\star, n_2^\star)$, and recall the definition (109). On the range $n \geq n^\star$, both inequalities (114) and (118) hold, and we obtain

$$\begin{aligned} & a_4(K_n)P_n + a_5(K_n) + 2(12)^6 K_n^{10} \cdot \frac{K_n^2}{P_n} \cdot \left(1 - \frac{12K_n^2}{P_n}\right)^{-1} \\ = \;& a_4(K_n)P_n + a_5^\star(K_n) + \left(-\frac{1}{240} + 2(12)^6 \cdot \frac{K_n^2}{P_n} \cdot \left(1 - \frac{12K_n^2}{P_n}\right)^{-1}\right) K_n^{10} \\ \leq \;& -K_n^4 P_n + a_5^\star(K_n) \end{aligned} \tag{119}$$

upon making use of (116). To conclude, set

$$L^\star := \limsup_{n \to \infty} \left(a_5^\star(K_n)\right) \tag{120}$$

and note that $L^\star$ is necessarily an element of $[-\infty, \infty)$, i.e., it is never the case that $L^\star = \infty$. This follows easily from the fact that the mapping $\mathbb{R}_+ \to \mathbb{R}_+ : x \to a_5^\star(x)$ is a polynomial of degree 10 whose leading coefficient $(-\frac{1}{240})$ is negative. As we recall (46) under (42)-(43), it is now plain from (119) that $L = -\infty$ by standard properties of the lim sup operation. ■

Careful inspection of the proof of Proposition 11.1 given at the end of Section 11 shows that the inequality (97) of Lemma 11.3 could be replaced without prejudice by the following weaker statement: For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (42)-(43), there exists some positive constant C such that

$$F(\theta_n) \leq C K_n^4 P_n^{4K_n - 3} \tag{121}$$

for all n sufficiently large in $\mathbb{N}_0$.

Now, from only the knowledge of the first four coefficients in Lemma 12.1 we can already conclude that

$$\lim_{P \to \infty} \frac{F(K,P)}{K^4 P^{4K-3}} = 1 \tag{122}$$

for *each* $K = 1, 2, \ldots$, so that for each $\varepsilon > 0$ there exists a finite integer $P^\star(\varepsilon, K)$ such that

$$F(K,P) \leq (1+\varepsilon) K^4 P^{4K-3}, \quad P \geq P^\star(\varepsilon, K) \tag{123}$$

Unfortunately, the threshold $P^\star(\varepsilon, K)$ is not known to be uniform with respect to K, and the approach does *not* necessarily imply (121) (with $C = 1+\varepsilon$) *unless* the sequence $K : \mathbb{N}_0 \to \mathbb{N}_0$ is bounded. This technical difficulty is at the root of why more information on the coefficients $a_4(K)$ and $a_5(K)$ (as provided in Lemma 12.1) is needed, and paves the way for the subsequent arguments behind Lemma 11.3.

References

[1] S.R. Blackburn and S. Gerke, "Connectivity of the uniform random intersection graph," *Discrete Mathematics* **309** (2009), pp. 5130-5140.

[2] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Transactions on Information Systems Security* **TISSEC 11** (2008), pp. 1-22.

[3] P. Erdős and A. Rényi, "On the evolution of random graphs," *Publ. Math. Inst. Hung. Acad. Sci.* **5** (1960), pp. 17-61.

[4] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the ACM Conference on Computer and Communications Security (2002), Washington (DC), November 2002.

[5] J. Fill, E.R. Scheinerman and K.B. Cohen-Singer, "Random intersection graphs when $m = \omega(n)$: An equivalence theorem relating the evolution of the $G(n, m, p)$ and $G(n, p)$ models," *Random Structures and Algorithms* **16** (2000), pp. 249-258.

[6] E. Godehardt and J. Jaworski "Two models of random intersection graphs for classification," in *Studies in Classification, Data Analysis and Knowledge Organization* **22**, Eds. O. Optiz and M. Schwaiger, Springer, Berlin (2003), pp. 67-82.

[7] E. Godehardt, J. Jaworski and K. Rybarczyk, "Random intersection graphs and classification," in *Studies in Classification, Data Analysis and Knowledge Organization* **33**, Eds. H.J. Lens and R,. Decker, Springer, Berlin (2007), pp. 67-74.

[8] S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, 2000.

[9] M.K. Karoński, E.R. Scheinerman, and K.B. Singer-Cohen, "On random intersection graphs: The subgraph problem," *Combinatorics, Probability and Computing* **8** (1999), pp. 131-159.

[10] P. Marbach, "A lower-bound on the number of rankings required in recommender systems using collaborativ filtering," Proceedings of the 42nd Annual Conference on Information Sciences and Systems (CISS 2008), Princeton University, Princeton (NJ), March 2008.

[11] M.D. Penrose, *Random Geometric Graphs*, Oxford Studies in Probability **5**, Oxford University Press, New York (NY), 2003.

[12] K. Rybarczyk "Diameter, connectivity and phase transition of the uniform random intersection graph," Submitted to *Discrete Mathematics*, July 2009.

[13] K.B. Singer, *Random Intersection Graphs*, Ph.D. Thesis, The Johns Hopkins University, Baltimore (MD), 1995.

[14] O. Yağan and A.M. Makowski, "On the random graph induced by a random key predistribution scheme under full visibility," In Proceedings of the IEEE International Symposium on Information Theory (ISIT 2008), Toronto (ON), June 2008.

[15] O. Yağan and A. M. Makowski, "Connectivity results for random key graphs," Proceedings of the IEEE International Symposium on Information Theory (ISIT 2009), Seoul (Korea), June 2009.

[16] O. Yağan and A.M. Makowski, "Zero-one laws for connectivity in random key graphs," Submitted to *Random Structures and Algorithms*, August 2009. Available online at arXiv:0908.3644v1 [math.CO]. Earlier draft available online (with a different title) at http://www.lib.umd.edu/drum/handle/1903/9403, January 2009.

[17] O. Yağan and A. M. Makowski, "On the existence of triangles in random key graphs," in the Proceedings of the Forty-Seventh Annual Allerton Conference on Communication, Control, and Computing, Monticello (IL), September 2009.

[18] O. Yağan and A. M. Makowski, "Random key graphs – Can they be small worlds?," submitted for inclusion in the program of the First Workshop on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks (GRAPH-HOC 2009), Chennai (India), December 2009.

A Establishing (49)

With positive integers K, P such that $3K \leq P$, we note that

$$\begin{aligned}
\frac{r(\theta)}{q(\theta)^2} &= \left(\frac{(P-2K)!}{(P-K)!}\right)^2 \cdot \frac{(P-2K)!}{(P-3K)!} \cdot \frac{P!}{(P-K)!} \\
&= \prod_{\ell=0}^{K-1} \left(\frac{P-2K-\ell}{P-K-\ell}\right) \cdot \prod_{\ell=0}^{K-1} \left(\frac{P-\ell}{P-K-\ell}\right) \\
&= \prod_{\ell=0}^{K-1} \left(1 - \left(\frac{K}{P-K-\ell}\right)^2\right), \qquad \text{(A.1)}
\end{aligned}$$

and elementary bounding arguments yield

$$\left(1 - \left(\frac{K}{P-2K}\right)^2\right)^K \leq \frac{r(\theta)}{q(\theta)^2} \leq \left(1 - \left(\frac{K}{P-K}\right)^2\right)^K.$$

Pick a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying the equivalent conditions (42)-(43) and consider n sufficiently large in $\mathbb{N}_0$ so that (47) holds with $c = 3$. On that range, as we replace θ by θ_n in the last chain of inequalities according to this scaling, we get

$$1 - \left(1 - \left(\frac{K_n}{P_n - K_n}\right)^2\right)^{K_n} \leq 1 - \frac{r(\theta_n)}{q(\theta_n)^2} \leq 1 - \left(1 - \left(\frac{K_n}{P_n - 2K_n}\right)^2\right)^{K_n}.$$

A standard sandwich argument will imply the desired equivalence (49) if we show that

$$1 - \left(1 - \left(\frac{K_n}{P_n - cK_n}\right)^2\right)^{K_n} \sim \frac{K_n^3}{P_n^2}, \quad c = 1, 2. \qquad \text{(A.2)}$$

To establish (A.2) we proceed as follows: Fix $c = 1, 2$ and on the appropriate range we note that

$$\begin{aligned}
&1 - \left(1 - \left(\frac{K_n}{P_n - cK_n}\right)^2\right)^{K_n} \\
&= \int_{1-\left(\frac{K_n}{P_n - cK_n}\right)^2}^{1} K_n t^{K_n - 1} dt \\
&= K_n \left(\frac{K_n}{P_n - cK_n}\right)^2 \int_0^1 \left(1 - \left(\frac{K_n}{P_n - cK_n}\right)^2 \tau\right)^{K_n - 1} d\tau \qquad \text{(A.3)}
\end{aligned}$$

after performing the simple change of variables $t = 1 - \left(\frac{K_n}{P_n - cK_n}\right)^2 \tau$.

Next we invoke (45) to find

$$\left(\frac{K_n}{P_n - cK_n}\right)^2 = \left(\frac{K_n}{P_n}(1 + o(1))\right)^2 = \frac{{K_n}^2}{{P_n}^2}(1 + o(1)), \tag{A.4}$$

so that

$$K_n \left(\frac{K_n}{P_n - cK_n}\right)^2 \sim \frac{K_n^3}{P_n^2}. \tag{A.5}$$

It is now plain from (A.3) and (A.5) that (A.2) holds provided

$$\lim_{n\to\infty} \int_0^1 \left(1 - \left(\frac{K_n}{P_n - cK_n}\right)^2 \tau\right)^{K_n - 1} d\tau = 1. \tag{A.6}$$

This is a consequence of the Bounded Convergence Theorem since

$$\lim_{n\to\infty} \left(1 - \left(\frac{K_n}{P_n - cK_n}\right)^2 \tau\right)^{K_n - 1} = 1, \quad 0 \le \tau \le 1$$

upon noting by elementary convergence results that

$$\lim_{n\to\infty} K_n \left(\frac{K_n}{P_n - cK_n}\right)^2 \tau = \lim_{n\to\infty} \left(\frac{K_n^2}{P_n}\right)\left(\frac{K_n}{P_n}\right)\tau = 0$$

across the range as a direct consequence of (43) and (45). ■

B Evaluating (63)–(64)

For notational convenience, we define

$$K_{ij} := [K_i(\theta) \cap K_j(\theta) \neq \emptyset].$$

for distinct $i, j = 1, 2, \ldots n$. Moreover, for any non-empty subset S of $\{1, \ldots, P\}$, we write

$$K_{Si} := [S \cap K_i(\theta) \neq \emptyset], \quad i = 1, \ldots, n.$$

In what follows we make repeated use of the decomposition (35). Beginning with the observation

$$\begin{aligned} &\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,124}(\theta)\right] \\ &\quad = \mathbb{P}\left[K_{12}, K_{13}, K_{23}, K_{14}, K_{24}\right] \\ &\quad = \mathbb{P}\left[K_{13}, K_{23}, K_{14}, K_{24}\right] - \mathbb{P}\left[K_{12}^c, K_{13}, K_{23}, K_{14}, K_{24}\right]. \end{aligned} \tag{B.1}$$

we shall compute each term in turn.

To compute the second term in (B.1) we condition on the sets K_1 and K_2 such that $K_1 \cap K_2 = \emptyset$. Thus,

$$\begin{aligned}
&\mathbb{P}\left[K_{12}^c, K_{13}, K_{23}, K_{14}, K_{24}\right] \\
&\quad = \sum_{|S|=|T|=K, S\cap T=\emptyset} \mathbb{P}\left[K_1 = S, K_2 = T, K_{S3}, K_{T3}, K_{S4}, K_{T4}\right] \\
&\quad = \sum_{|S|=|T|=K, S\cap T=\emptyset} \mathbb{P}\left[K_1 = S, K_2 = T\right] \mathbb{P}\left[K_{S3}, K_{T3}, K_{S4}, K_{T4}\right] \\
&\quad = \sum_{|S|=|T|=K, S\cap T=\emptyset} \binom{P}{K}^{-2} \mathbb{P}\left[K_{S3}, K_{T3}\right] \cdot \mathbb{P}\left[K_{S4}, K_{T4}\right] \\
&\quad = \sum_{|S|=|T|=K, S\cap T=\emptyset} \binom{P}{K}^{-2} \left(\mathbb{P}\left[K_{S3}, K_{T3}\right]\right)^2 \\
&\quad = \binom{P}{K}^{-2} \sum_{|S|=|T|=K, S\cap T=\emptyset} \left(\mathbb{P}\left[K_{S3}\right] - \mathbb{P}\left[K_{T3}^c\right] + \mathbb{P}\left[K_{S3}^c, K_{T3}^c\right]\right)^2 \\
&\quad = \binom{P}{K}^{-2} \sum_{|S|=|T|=K, S\cap T=\emptyset} \left(1 - \mathbb{P}\left[K_{S3}^c\right] - \mathbb{P}\left[K_{T3}^c\right] + \mathbb{P}\left[K_{S3}^c, K_{T3}^c\right]\right)^2 \\
&\quad = \binom{P}{K}^{-2} \sum_{|S|=|T|=K, S\cap T=\emptyset} \left(1 - 2q(\theta) + r(\theta)\right)^2 \\
&\quad = \binom{P}{K}^{-2} \binom{P}{K} \binom{P-K}{K} \left(1 - 2q(\theta) + r(\theta)\right)^2 \\
&\quad = q(\theta)\left(1 - 2q(\theta) + r(\theta)\right)^2 \qquad \text{(B.2)}
\end{aligned}$$

as we note from (5) that $\mathbb{P}\left[K_{S3}^c\right] = \mathbb{P}\left[K_{T3}^c\right] = q(\theta)$ for S and T in $\mathcal{P}_K$ with $\mathbb{P}\left[K_{S3}^c, K_{T3}^c\right] = r(\theta)$ whenever $S \cap T = \emptyset$.

We now turn to the first term in (B.1). Again, upon making repeated use of (35) we find

$$\begin{aligned}
&\mathbb{P}\left[K_{13}, K_{23}, K_{14}, K_{24}\right] \\
&\quad = \mathbb{P}\left[K_{23}, K_{14}, K_{24}\right] - \mathbb{P}\left[K_{13}^c, K_{23}, K_{14}, K_{24}\right] \\
&\quad = \mathbb{P}\left[K_{14}, K_{24}\right] - \mathbb{P}\left[K_{23}^c, K_{14}, K_{24}\right] - \mathbb{P}\left[K_{13}^c, K_{14}, K_{24}\right] + \mathbb{P}\left[K_{13}^c, K_{23}^c, K_{14}, K_{24}\right] \\
&\quad = \left(1 - q(\theta)\right)^2 - 2\mathbb{P}\left[K_{23}^c, K_{14}, K_{24}\right] + \mathbb{P}\left[K_{13}^c, K_{23}^c, K_{24}\right] - \mathbb{P}\left[K_{13}^c, K_{23}^c, K_{14}^c, K_{24}\right] \\
&\quad = \left(1 - q(\theta)\right)^2 - 2\mathbb{P}\left[K_{23}^c, K_{14}, K_{24}\right] + \mathbb{P}\left[K_{13}^c, K_{23}^c, K_{24}\right] \\
&\qquad - \mathbb{P}\left[K_{13}^c, K_{23}^c, K_{14}^c\right] + \mathbb{P}\left[K_{13}^c, K_{23}^c, K_{14}^c, K_{24}^c\right] \qquad \text{(B.3)}
\end{aligned}$$

as we note that $\mathbb{P}\left[K_{23}^c, K_{14}, K_{24}\right] = \mathbb{P}\left[K_{13}^c, K_{14}, K_{24}\right]$. Next, we find

$$\begin{aligned}
\mathbb{P}\left[K_{23}^c, K_{14}, K_{24}\right] &= \sum_{|S|=K} \mathbb{P}\left[K_4 = S, K_{23}^c, K_{S1}, K_{S2}\right] \\
&= \sum_{|S|=K} \mathbb{P}\left[K_4 = S\right] \mathbb{P}\left[K_{23}^c, K_{S1}, K_{S2}\right] \\
&= \sum_{|S|=K} \binom{P}{K}^{-1} \mathbb{P}\left[K_{S1}\right] \cdot \mathbb{P}\left[K_{23}^c, K_{S2}\right] \\
&= \sum_{|S|=K} \binom{P}{K}^{-1} (1-q(\theta)) \cdot q(\theta)(1-q(\theta)) \quad \text{(B.4)} \\
&= q(\theta)(1-q(\theta))^2 \quad \text{(B.5)}
\end{aligned}$$

upon using (36) in (B.4).

In a similar manner, we obtain

$$\begin{aligned}
\mathbb{P}\left[K_{13}^c, K_{23}^c, K_{24}\right] &= \sum_{|S|=K} \mathbb{P}\left[K_2 = S, K_{13}^c, K_{S3}^c, K_{S4}\right] \\
&= \sum_{|S|=K} \mathbb{P}\left[K_2 = S\right] \mathbb{P}\left[K_{13}^c, K_{S3}^c, K_{S4}\right] \\
&= \sum_{|S|=K} \binom{P}{K}^{-1} \mathbb{P}\left[K_{S4}\right] \cdot \mathbb{P}\left[K_{13}^c, K_{S3}^c\right] \\
&= \sum_{|S|=K} \binom{P}{K}^{-1} (1-q(\theta)) \cdot q(\theta)^2 \quad \text{(B.6)} \\
&= q(\theta)^2(1-q(\theta)) \quad \text{(B.7)}
\end{aligned}$$

where (B.6) follows from (37).

We also get

$$\begin{aligned}
\mathbb{P}\left[K_{13}^c, K_{23}^c, K_{14}^c\right] &= \sum_{|S|=K} \mathbb{P}\left[K_1 = S, K_{S3}^c, K_{23}^c, K_{S4}^c\right] \\
&= \sum_{|S|=K} \mathbb{P}\left[K_1 = S\right] \mathbb{P}\left[K_{S3}^c, K_{23}^c, K_{S4}^c\right] \\
&= \sum_{|S|=K} \binom{P}{K}^{-1} \mathbb{P}\left[K_{S4}^c\right] \cdot \mathbb{P}\left[K_{S3}^c, K_{23}^c\right]
\end{aligned}$$

$$= \sum_{|S|=K} \binom{P}{K}^{-1} q(\theta) \cdot q(\theta)^2$$
$$= q(\theta)^3. \tag{B.8}$$

Finally consider the term $\mathbb{P}[K_{13}^c, K_{23}^c, K_{14}^c, K_{24}^c]$: By conditioning on the cardinality of the intersection $K_1 \cap K_2$, we obtain

$$\begin{aligned}
&\mathbb{P}[K_{13}^c, K_{23}^c, K_{14}^c, K_{24}^c] \\
&= \sum_{|S|=|T|=K} \mathbb{P}[K_1 = S, K_2 = T, K_{S3}^c, K_{T3}^c, K_{S4}^c, K_{T4}^c] \\
&= \sum_{|S|=K} \sum_{k=0}^{K} \sum_{|T|=K, |T\cap S|=k} \mathbb{P}[K_1 = S, K_2 = T, K_{S3}^c, K_{T3}^c, K_{S4}^c, K_{T4}^c] \\
&= \sum_{k=0}^{K} c_k(\theta)
\end{aligned} \tag{B.9}$$

where for each $k = 0, 1, \ldots, K$, we have set

$$\begin{aligned}
c_k(\theta) &:= \sum_{|S|=|T|=K, |T\cap S|=k} \mathbb{P}[K_1 = S, K_2 = T, K_{S3}^c, K_{T3}^c, K_{S4}^c, K_{T4}^c] \qquad \text{(B.10)} \\
&= \sum_{|S|=|T|=K, |T\cap S|=k} \mathbb{P}[K_1 = S]\, \mathbb{P}[K_2 = T]\, \mathbb{P}[K_{S3}^c, K_{T3}^c] \cdot \mathbb{P}[K_{S4}^c, K_{T4}^c] \\
&= \sum_{|S|=K} \mathbb{P}[K_1 = S] \sum_{|T|=K, |T\cap S|=k} \mathbb{P}[K_2 = T]\, \mathbb{P}[K_{S3}^c, K_{T3}^c] \cdot \mathbb{P}[K_{S4}^c, K_{T4}^c] \\
&= \sum_{|S|=K} \binom{P}{K}^{-1} \sum_{|T|=K, |T\cap S|=k} \binom{P}{K}^{-1} \mathbb{P}[K_{S3}^c, K_{T3}^c] \cdot \mathbb{P}[K_{S4}^c, K_{T4}^c] \\
&= \sum_{|S|=K} \binom{P}{K}^{-1} \sum_{|T|=K, |T\cap S|=k} \binom{P}{K}^{-1} \left(\frac{\binom{P-2K+k}{K}}{\binom{P}{K}} \right)^2 \\
&= \sum_{|S|=K} \binom{P}{K}^{-1} \cdot \binom{K}{k} \binom{P-K}{K-k} \cdot \binom{P}{K}^{-1} \left(\frac{\binom{P-2K+k}{K}}{\binom{P}{K}} \right)^2 \qquad \text{(B.11)}
\end{aligned}$$

and the expression follows (64).

Substituting (B.2) and (B.3) (with the help of (B.5), (B.7), (B.8) and (B.11)) into (B.1), we find

$$\mathbb{E}[\chi_{n,123}(\theta)\chi_{n,124}(\theta)]$$

$$
\begin{aligned}
&= (1-q(\theta))^2 - 2q(\theta)(1-q(\theta))^2 + q(\theta)^2(1-q(\theta)) - q(\theta)^3 \\
&\quad -q(\theta)\left(1-2q(\theta)+r(\theta)\right)^2 + \sum_{k=0}^{K} c_k(\theta) \qquad \text{(B.12)}
\end{aligned}
$$

where we have used the notation (64).

As we seek to simplify this last expression, we note that

$$
\begin{aligned}
&(1-q(\theta))^2 - 2q(\theta)(1-q(\theta))^2 + q(\theta)^2(1-q(\theta)) - q(\theta)^3 \\
&\quad = (1-q(\theta))^2\left(1-2q(\theta)\right) + q(\theta)^2(1-q(\theta)) - q(\theta)^3 \\
&\quad = (1-q(\theta))^2\left(1-2q(\theta)+q(\theta)^2\right) - q(\theta)^2(1-q(\theta))^2 \\
&\qquad + q(\theta)^2(1-q(\theta)) - q(\theta)^3 \\
&\quad = (1-q(\theta))^4 + q(\theta)^2\left((1-q(\theta)) - (1-q(\theta))^2\right) - q(\theta)^3 \\
&\quad = (1-q(\theta))^4 + q(\theta)^2(1-q(\theta))\left(1-(1-q(\theta))\right) - q(\theta)^3 \\
&\quad = (1-q(\theta))^4 + q(\theta)^3(1-q(\theta)) - q(\theta)^3 \\
&\quad = (1-q(\theta))^4 - q(\theta)^4. \qquad \text{(B.13)}
\end{aligned}
$$

Next, we observe that

$$
\begin{aligned}
&q(\theta)\left(1-2q(\theta)+r(\theta)\right)^2 \\
&\quad = q(\theta)\left(1-2q(\theta)+q(\theta)^2-q(\theta)^2+r(\theta)\right)^2 \\
&\quad = q(\theta)\left((1-q(\theta))^2 - \left(q(\theta)^2-r(\theta)\right)\right)^2 \\
&\quad = q(\theta)\left((1-q(\theta))^4 - 2\left(1-q(\theta)\right)^2\left(q(\theta)^2-r(\theta)\right) + \left(q(\theta)^2-r(\theta)\right)^2\right) \\
&\quad = q(\theta)\left(1-q(\theta)\right)^4 - 2q(\theta)\left(1-q(\theta)\right)^2\left(q(\theta)^2-r(\theta)\right) \\
&\qquad + q(\theta)\left(q(\theta)^2-r(\theta)\right)^2. \qquad \text{(B.14)}
\end{aligned}
$$

Subtracting (B.14) from (B.13) gives

$$
\begin{aligned}
&(1-q(\theta))^4 - q(\theta)^4 - q(\theta)\left(1-2q(\theta)+r(\theta)\right)^2 \\
&\quad = (1-q(\theta))^4 - q(\theta)^4 - q(\theta)\left(1-q(\theta)\right)^4 + 2q(\theta)\left(1-q(\theta)\right)^2\left(q(\theta)^2-r(\theta)\right) \\
&\qquad - q(\theta)\left(q(\theta)^2-r(\theta)\right)^2 \\
&\quad = (1-q(\theta))^4\left(1-q(\theta)\right) - q(\theta)^4 + 2q(\theta)\left(1-q(\theta)\right)^2\left(q(\theta)^2-r(\theta)\right) \\
&\qquad - q(\theta)\left(q(\theta)^2-r(\theta)\right)^2 \\
&\quad = (1-q(\theta))^5 - q(\theta)^4 + 2q(\theta)\left(1-q(\theta)\right)^2\left(q(\theta)^2-r(\theta)\right) \\
&\qquad - q(\theta)\left(q(\theta)^2-r(\theta)\right)^2. \qquad \text{(B.15)}
\end{aligned}
$$

Reporting the outcome of this last calculation into (B.12) we then get

$$\begin{aligned}
&\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,124}(\theta)\right] \\
&\quad = \quad (1-q(\theta))^5 + 2q(\theta)\,(1-q(\theta))^2\left(q(\theta)^2 - r(\theta)\right) \\
&\qquad\quad - q(\theta)\left(q(\theta)^2 - r(\theta)\right)^2 + \sum_{k=0}^{K} c_k(\theta) - q(\theta)^4, \qquad \text{(B.16)}
\end{aligned}$$

and the conclusion (63) follows as we make use of the expression (26) for $\beta(\theta)$.

C Proofs of Lemma 12.1 and Lemma 12.2

The proofs of both Lemma 12.1 and Lemma 12.2 will make use of the following observations: Pick positive integers K and P such that $K \geq 4$ and $3K \leq P$, and recall the expressions (101) and (102) appearing in (103).

Fix $k = 0, 1, \ldots, 4$. The product

$$b_{K,k}(\theta) = \prod_{i=1}^{K}(P - 3K + k + i) \cdot \prod_{j=1}^{3K-k}(P - 3K + k + j) \qquad \text{(C.1)}$$

has $K + (3K - k) = 4K - k$ factors, hence defines a polynomial expression in P with leading term P^{4K-k}, say

$$b_{K,k}(P) = \sum_{\ell=0}^{4K-k} \beta_{k,\ell}(K) P^{\ell} \qquad \text{(C.2)}$$

for some integer coefficients $\beta_{k,0}(K), \ldots, \beta_{k,4K-k}(K)$ with $\beta_{k,4K-k}(K) = 1$. On the other hand, the expression

$$b_K(\theta) = \left(\prod_{i=1}^{K}(P - 2K + i)\right)^4 = \left(\prod_{i=K}^{2K-1}(P - i)\right)^4 \qquad \text{(C.3)}$$

is a product of $4K$ factors with leading term P^{4K}, and we can write it as a polynomial in P, namely

$$b_K(P) = \sum_{\ell=0}^{4K} \beta_{\ell}(K) P^{\ell} \qquad \text{(C.4)}$$

for some integer coefficients $\beta_0(K), \ldots, \beta_{4K}(K)$ with $\beta_{4K}(K) = 1$.

Direct substitution followed by elementary manipulations gives

$$\begin{aligned}
&\sum_{k=0}^{4} k!\binom{K}{k}^2 \cdot b_{K,k}(\theta) \\
&\quad = \sum_{k=0}^{4} k!\binom{K}{k}^2 \cdot \left(\sum_{\ell=0}^{4K-k} \beta_{k,\ell}(K) P^\ell \right) \\
&\quad = \sum_{k=0}^{4} k!\binom{K}{k}^2 \cdot \left(\sum_{\ell=0}^{4K-5} \beta_{k,\ell}(K) P^\ell + \sum_{\ell=4K-4}^{4K-k} \beta_{k,\ell}(K) P^\ell \right) \\
&\quad = \sum_{\ell=0}^{4K} \left(\sum_{k=0}^{\min(4K-\ell,4)} k!\binom{K}{k}^2 \beta_{k,\ell}(K) \right) P^\ell,
\end{aligned}$$

and it is then plain that

$$\begin{aligned}
F(\theta) &= \sum_{k=0}^{4} k!\binom{K}{k}^2 \cdot b_{K,k}(\theta) - b(\theta) \\
&= \sum_{\ell=0}^{4K} \left(\sum_{k=0}^{\min(4K-\ell,4)} k!\binom{K}{k}^2 \beta_{k,\ell}(K) \right) P^\ell - \sum_{\ell=0}^{4K} \beta_\ell(K) P^\ell.
\end{aligned}$$

Finally, upon comparing with (104) we get the relations

$$a_\ell(K) = \left(\sum_{k=0}^{\min(\ell,4)} k!\binom{K}{k}^2 \beta_{k,4K-\ell}(K) \right) - \beta_{4K-\ell}(K) \tag{C.5}$$

for all $\ell = 0, \ldots, 4K$.

C.1 A proof of Lemma 12.2

We begin with some simple observations: For some positive integer M, consider the mapping $R : \mathbb{R} \to \mathbb{R}$ given by

$$R(x) = \prod_{m=1}^{M} (x - r_m), \quad x \in \mathbb{R}$$

with scalars $r_1, \ldots, r_M$, not necessarily distinct. Obviously, $R : \mathbb{R} \to \mathbb{R}$ is a polynomial (in the variable x) of degree M with all its roots located at

$r_1, \ldots, r_M$. It can be written in the form

$$R(x) = \sum_{m=0}^{M} \rho_{M-m} x^m, \quad x \in \mathbb{R} \tag{C.6}$$

for some coefficients $\rho_0, \ldots, \rho_M$ with $\rho_0 = 1$; these coefficients are uniquely determined by the roots $r_1, \ldots, r_M$. In fact, for each $m = 0, 1, \ldots, M$, the coefficient ρ_m of x^{M-m} is given by

$$\rho_m = (-1)^m \sum\nolimits_{(k_1,\ldots,k_m)\in\mathcal{M}_m} r_{k_1} \ldots r_{k_m} \tag{C.7}$$

where $\mathcal{M}_m$ denotes the collection of all unordered m-uples drawn without repetition from the set of indices $1, \ldots, M$. Obviously $|\mathcal{M}_m| = \binom{M}{m}$ and the bounds

$$|\rho_m| \leq \binom{M}{m} \cdot (r^\star)^m \leq (M r^\star)^m \tag{C.8}$$

hold with $r^\star$ given by

$$r^\star := \max\left(|r_m|,\ m = 1, \ldots, M\right). \tag{C.9}$$

Now we turn to the proof of Lemma 12.2: Pick positive integers K and P such that $K \geq 4$ and $3K \leq P$, and fix $\ell = 4, 5, \ldots, 4K$ – We shall give a proof only in that range for simplicity of exposition; after all the desired bounds are already implied by the exact expression for $a_0(K), \ldots, a_3(K)$ given as part of Lemma 12.1. On the range $\ell = 4, \ldots, 4K$, the bound (C.5) already implies

$$|a_\ell(K)| \leq \left(\sum_{k=0}^{4} k! \binom{K}{k}^2 |\beta_{k,4K-\ell}(K)| \right) + |\beta_{4K-\ell}(K)|. \tag{C.10}$$

For each $k = 0, 1, \ldots, 4$, we note that

$$k! \binom{K}{k}^2 \leq k! \left(\frac{K^k}{k!}\right)^2 = \frac{K^{2k}}{k!}. \tag{C.11}$$

We then apply the bound (C.8)-(C.9) to the polynomal $b_{K,k}$: From (C.1) we get the values $M = 4K - k$ and $r^\star = 3K - (k+1)$, Also, we note that $\beta_{k,4K-\ell}(K)$ is the coefficient of $P^{4K-\ell}$ (thus of $P^{4K-k-(\ell-k)}$) in the polynomial $b_{K,k}(P)$ of order $4K - k$. Therefore, applying the bound (C.8)-(C.9) we find

$$\begin{aligned} |\beta_{k,4K-\ell}(K)| &\leq \left((4K-k)\cdot(3K-(k+1))\right)^{\ell-k} \\ &\leq \left(12K^2\right)^{\ell-k}. \end{aligned} \tag{C.12}$$

In a similar way, we apply the bound (C.8)-(C.9) to the polynomial b_K. This time, (C.3) gives $M = 4K$ and $r^\star = 2K - 1$, and we conclude that

$$|\beta_{4K-\ell}(K)| \leq (4K)^\ell \cdot (2K-1)^\ell \leq \left(8K^2\right)^\ell . \tag{C.13}$$

Collecting the bounds (C.11), (C.12) and (C.13) we see from (C.10) that

$$\begin{aligned} |a_\ell(K)| &\leq \sum_{k=0}^{4} \frac{K^{2k}}{k!} \cdot \left(12K^2\right)^{\ell-k} + \left(8K^2\right)^\ell . \\ &= C_\ell \left(12K^2\right)^\ell \end{aligned} \tag{C.14}$$

with

$$C_\ell := \sum_{k=0}^{4} \frac{1}{k! \cdot 12^k} + \left(\frac{8}{12}\right)^\ell .$$

It is a simple matter to check that $C_\ell \leq 2$. ■

C.2 A proof of Lemma 12.1

The basis for the proof can be found in the expression (C.5) for the coefficients $a_0(K), \ldots, a_{4K}(K)$.

For $\ell = 0$, this expression becomes

$$a_0(K) = \beta_{0,4K}(K) - \beta_{4K}(K) = 1 - 1 = 0.$$

For $\ell = 1$, we get

$$\begin{aligned} a_1(K) &= \beta_{0,4K-1}(K) + K^2\beta_{1,4K-1}(K) - \beta_{4K-1}(K) \\ &= -\sum_{\ell=1}^{K}(3K-\ell) - \sum_{j=1}^{3K}(3K-j) + K^2 - \left(-4\sum_{i=K}^{2K-1} i\right) = 0 \end{aligned}$$

where we have used the formula (C.7) to evaluate $\beta_{0,4K-1}(K)$ and $\beta_{4K-1}(K)$.

For $\ell = 2$, this approach yields

$$\begin{aligned} &a_2(K) \\ &= \beta_{0,4K-2}(K) + K^2\beta_{1,4K-2}(K) + \frac{K^2(K-1)^2}{2}\beta_{2,4K-2}(K) - \beta_{4K-2}(K) \\ &= \beta_{0,4K-2}(K) + K^2\beta_{1,4K-2}(K) + \frac{K^2(K-1)^2}{2} - \beta_{4K-2}(K) \end{aligned}$$

and this leads to

$$\begin{aligned} a_2(K) &= \sum_{i=1}^{3K-2} i \sum_{j=i+1}^{3K-1} j + \sum_{i=2K}^{3K-2} i \sum_{j=i+1}^{3K-1} j + \left(\sum_{i=2K}^{3K-1} i\right)\left(\sum_{i=1}^{3K-1} i\right) \\ &\quad - K^2 \left(\sum_{i=1}^{3K-2} i + \sum_{i=2K-1}^{3K-2} i\right) + \frac{K^2(K-1)^2}{2} \\ &\quad - \left(\binom{4}{1}^2 \cdot \sum_{i=K}^{2K-2} i \sum_{j=i+1}^{2K-1} j + \binom{4}{2} \sum_{i=K}^{2K-1} i^2\right) \\ &= 0. \end{aligned} \tag{C.15}$$

For $\ell = 3$, straightforward computations give

$$\begin{aligned} & a_3(K) \\ &= - \left(\sum_{v=1}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j + \sum_{v=2K}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j\right) \\ &\quad - \left(\sum_{i=1}^{3K-1} i \cdot \sum_{i=2K}^{3K-2} i \sum_{j=i+1}^{3K-1} j + \sum_{i=2K}^{3K-1} i \cdot \sum_{i=1}^{3K-2} i \sum_{j=i+1}^{3K-1} j\right) \\ &\quad + K^2 \left(\sum_{i=1}^{3K-3} i \sum_{j=i+1}^{3K-2} j + \sum_{i=2K-1}^{3K-3} i \sum_{j=i+1}^{3K-2} j + \left(\sum_{i=2K-1}^{3K-2} i\right)\left(\sum_{i=1}^{3K-2} i\right)\right) \\ &\quad - \frac{K^2(K-1)^2}{2} \left(\sum_{i=1}^{3K-3} i + \sum_{i=2K-2}^{3K-3} i\right) + \frac{K^2(K-1)^2(K-2)^2}{6} \\ &\quad + \binom{4}{1}^3 \cdot \sum_{v=K}^{2K-3} v \sum_{i=v+1}^{2K-2} i \sum_{j=i+1}^{2K-1} j + \binom{4}{2}\binom{4}{1} \sum_{j=K}^{2K-1} j^2 \left(\sum_{i=K}^{2K-1} i - j\right) \\ &\quad + \binom{4}{3} \sum_{i=K}^{2K-1} i^3 \\ &= K^4 \end{aligned} \tag{C.16}$$

as announced.

For $a_4(K)$, we proceed in a similar manner to get[1]

$$a_4(K) \tag{C.17}$$

[1]Evaluating the expression (C.17) (as well as (C.18) given next) by hand is quite cumbersome. To avoid this, one can make use of a computer software (e.g., Mathematica, MATLAB) that can perform computations symbolically.

$$
\begin{aligned}
= \quad & \sum_{l=1}^{3K-4} l \sum_{v=l+1}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j + \sum_{l=2K}^{3K-4} l \sum_{v=l+1}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j \\
& + \sum_{i=1}^{3K-1} i \cdot \sum_{v=2K}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j + \sum_{i=2K}^{3K-1} i \cdot \sum_{v=1}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j \\
& + \left(\sum_{i=1}^{3K-2} i \sum_{j=i+1}^{3K-1} j \right) \left(\sum_{i=2K}^{3K-2} i \sum_{j=i+1}^{3K-1} j \right) - K^2 \sum_{v=1}^{3K-4} v \sum_{i=v+1}^{3K-3} i \sum_{j=i+1}^{3K-2} j \\
& - K^2 \left(\sum_{v=2K-1}^{3K-4} v \sum_{i=v+1}^{3K-3} i \sum_{j=i+1}^{3K-2} j + \sum_{i=1}^{3K-2} i \cdot \sum_{i=2K-1}^{3K-3} i \sum_{j=i+1}^{3K-2} j \right) \\
& - K^2 \sum_{i=2K-1}^{3K-2} i \cdot \sum_{i=1}^{3K-3} i \sum_{j=i+1}^{3K-2} j + \frac{K^2(K-1)^2}{2} \sum_{i=1}^{3K-4} i \sum_{j=i+1}^{3K-3} j \\
& + \frac{K^2(K-1)^2}{2} \left(\sum_{i=2K-2}^{3K-4} i \sum_{j=i+1}^{3K-3} j + \left(\sum_{i=2K-2}^{3K-3} i \right) \left(\sum_{j=1}^{3K-3} j \right) \right) \\
& - \frac{K^2(K-1)^2(K-2)^2}{6} \left(\sum_{i=1}^{3K-4} i + \sum_{i=2K-3}^{3K-4} i \right) \\
& + \frac{K^2(K-1)^2(K-2)^2(K-3)^2}{24} - \binom{4}{1}^4 \cdot \sum_{l=K}^{2K-4} l \sum_{v=K+1}^{2K-3} v \sum_{i=v+1}^{2K-2} i \sum_{j=i+1}^{2K-1} j \\
& - \binom{4}{2} \binom{4}{1}^2 \cdot \sum_{v=K}^{2K-1} v^2 \left(\sum_{i=K}^{2K-2} i \sum_{j=i+1}^{2K-1} j - v \sum_{i=K}^{2K-1} i + v^2 \right) \\
& - \binom{4}{3} \binom{4}{1} \sum_{j=K}^{2K-1} j^3 \left(\sum_{i=K}^{2K-1} i - j \right) - \binom{4}{2}^2 \cdot \sum_{i=K}^{2K-2} i^2 \sum_{j=i+1}^{2K-1} j^2 - \sum_{i=K}^{2K-1} i^4 \\
= \quad & -6K^6 + 6K^5 - K^4.
\end{aligned}
$$

Finally, $a_5(K)$ is given by

$$
\begin{aligned}
& a_5(K) \qquad\qquad \text{(C.18)} \\
= \quad & - \sum_{u=1}^{3K-5} u \sum_{l=u+1}^{3K-4} l \sum_{v=l+1}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j \\
& - \sum_{u=2K}^{3K-5} u \sum_{l=u+1}^{3K-4} l \sum_{v=l+1}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j
\end{aligned}
$$

$$
\begin{aligned}
&- \sum_{i=1}^{3K-1} i \cdot \sum_{l=2K}^{3K-4} l \sum_{v=l+1}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j \\
&- \sum_{i=2K}^{3K-1} i \cdot \sum_{l=1}^{3K-4} l \sum_{v=l+1}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j \\
&- \left(\sum_{v=1}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j \right) \left(\sum_{i=2K}^{3K-2} i \sum_{j=i+1}^{3K-1} j \right) \\
&- \left(\sum_{v=2K}^{3K-3} v \sum_{i=v+1}^{3K-2} i \sum_{j=i+1}^{3K-1} j \right) \left(\sum_{i=1}^{3K-2} i \sum_{j=i+1}^{3K-1} j \right) \\
&+ K^2 \left(\sum_{l=1}^{3K-5} l \sum_{v=l+1}^{3K-4} v \sum_{i=v+1}^{3K-3} i \sum_{j=i+1}^{3K-2} j + \sum_{l=2K-1}^{3K-5} l \sum_{v=l+1}^{3K-4} v \sum_{i=v+1}^{3K-3} i \sum_{j=i+1}^{3K-2} j \right) \\
&+ K^2 \sum_{i=1}^{3K-2} i \cdot \sum_{v=2K-1}^{3K-4} v \sum_{i=v+1}^{3K-3} i \sum_{j=i+1}^{3K-2} j \\
&+ K^2 \sum_{i=2K-1}^{3K-2} i \cdot \sum_{v=1}^{3K-4} v \sum_{i=v+1}^{3K-3} i \sum_{j=i+1}^{3K-2} j \\
&+ K^2 \left(\sum_{i=1}^{3K-3} i \sum_{j=i+1}^{3K-2} j \right) \left(\sum_{i=2K-1}^{3K-3} i \sum_{j=i+1}^{3K-2} j \right) \\
&- \frac{K^2(K-1)^2}{2} \left(\sum_{v=1}^{3K-5} v \sum_{i=v+1}^{3K-4} i \sum_{j=i+1}^{3K-3} j + \sum_{v=2K-2}^{3K-5} v \sum_{i=v+1}^{3K-4} i \sum_{j=i+1}^{3K-3} j \right) \\
&- \frac{K^2(K-1)^2}{2} \left(\sum_{i=1}^{3K-3} i \cdot \sum_{i=2K-2}^{3K-4} i \sum_{j=i+1}^{3K-3} j + \sum_{i=2K-2}^{3K-3} i \cdot \sum_{i=1}^{3K-4} i \sum_{j=i+1}^{3K-3} j \right) \\
&+ \frac{K^2(K-1)^2(K-2)^2}{6} \left(\sum_{i=1}^{3K-5} i \sum_{j=i+1}^{3K-4} j + \sum_{i=2K-3}^{3K-5} i \sum_{j=i+1}^{3K-4} j \right) \\
&+ \frac{K^2(K-1)^2(K-2)^2}{6} \sum_{i=1}^{3K-4} i \cdot \sum_{i=2K-3}^{3K-4} j \\
&- \frac{K^2(K-1)^2(K-2)^2(K-3)^2}{24} \left(\sum_{i=1}^{3K-5} i + \sum_{i=2K-4}^{3K-5} i \right)
\end{aligned}
$$

$$
\begin{aligned}
&+\binom{4}{1}^5 \cdot \sum_{u=K}^{2K-5} u \sum_{l=u+1}^{2K-4} l \sum_{v=K+1}^{2K-3} v \sum_{i=v+1}^{2K-2} i \sum_{j=i+1}^{2K-1} j \\
&+\binom{4}{2}\binom{4}{1}^3 \\
&\quad \times \sum_{l=K}^{2K-1} l^2 \left(\sum_{v=K}^{2K-3} v \sum_{i=m+1}^{2K-2} i \sum_{j=i+1}^{2K-1} j - l \sum_{i=K}^{2K-2} i \sum_{j=i+1}^{2K-1} j + l^2 \sum_{i=K}^{2K-1} -l^3 \right) \\
&+\binom{4}{2}^2\binom{4}{1} \cdot \sum_{v=K}^{2K-1} v \left(\sum_{i=K}^{2K-2} i^2 \sum_{j=i+1}^{2K-1} j^2 - v^2 \sum_{i=K}^{2K-1} i^2 + v^4 \right) \\
&+\binom{4}{3}\binom{4}{2} \sum_{i=K}^{2K-1} i^3 \left(\sum_{j=K}^{2K-1} j^2 - i^2 \right) \\
&+\binom{4}{3}\binom{4}{1}^2 \cdot \sum_{v=K}^{2K-1} v^3 \left(\sum_{i=K}^{2K-2} i \sum_{j=i+1}^{2K-1} j - v \sum_{i=K}^{2K-1} + v^2 \right) \\
&+\binom{4}{4}\binom{4}{1} \sum_{i=K}^{2K-1} i^4 \left(\sum_{j=K}^{2K-1} j - i \right) \\
= \quad & -\frac{1}{120}K^{10} + \frac{1}{6}K^9 + \frac{199}{12}K^8 - 34K^7 + \frac{1207}{120}K^6 + \frac{161}{6}K^5 \\
& - \frac{209}{6}K^4 + 20K^3 - \frac{24}{5}K^2.
\end{aligned}
$$

■